

09/404,547

日 本 国 特 許 庁

PATENT OFFICE  
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日

Date of Application:

1998年 9月30日

出 願 番 号

Application Number:

平成10年特許願第292824号

出 願 人

Applicant(s):

株式会社東芝

RECEIVED

FEB 16 2000

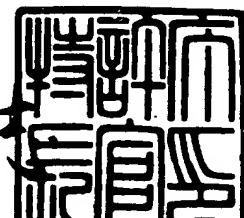
GROUP 2700

CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年 4月16日

特許庁長官  
Commissioner,  
Patent Office

伴佐山 建



【書類名】 特許願

【整理番号】 A009806136

【提出日】 平成10年 9月30日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00

【発明の名称】 中継装置及び通信装置

【請求項の数】 21

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

【氏名】 斉藤 健

【発明者】

【住所又は居所】 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内

【氏名】 高畠 由彰

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705037

【書類名】 明細書  
【発明の名称】 中継装置及び通信装置  
【特許請求の範囲】

【請求項 1】

第 1 のネットワークに接続された第 1 のインタフェース手段と、

第 2 のネットワークに接続された第 2 のインタフェース手段と、

前記第 2 のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第 1 のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第 1 の情報を、代理で受信し、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットへの第 2 の情報に変換して、送信する代理構成手段と、

前記第 1 のネットワーク上の装置からの前記第 1 の情報を受信した際、この情報が少なくとも所定の情報であるか否かを検出する検出手段と、

前記検出手段により、検出した第 1 の情報が前記所定の情報であった場合には、前記所定の情報を前記第 2 のネットワーク上の装置またはサービスまたはサブユニットに転送する転送手段とを具備したことを特徴とする中継装置。

【請求項 2】

前記所定の情報は、前記第 1 のネットワーク上の装置と前記第 2 のネットワーク上の装置またはサービスまたはサブユニット間で送受信される情報を保護するための情報であり、少なくとも認証手続きに関する情報からなることを特徴とする請求項 1 に記載の中継装置。

【請求項 3】

前記第 1 のインタフェース手段または前記第 2 のインタフェース手段から特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第 1 のインタフェース手段または前記第 2 のインタフェース手段の一方から受信された前記特定のコンテンツを含むデータを、前記第 1 のインタフェース手段または前記第 2 のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備したことを特徴とする請求項 2 に記載の中継装置。

【請求項 4】

第1のネットワークに接続された第1のインタフェース手段と、

第2のネットワークに接続された第2のインタフェース手段と、

前記第2のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第1の情報を、代理で受信し、前記第2のネットワーク上の装置またはサービスまたはサブユニットへの第2の情報に変換して、送信する代理構成手段と、

前記第1のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第1のコピープロテクション処理手段と、

前記第2のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第2のコピープロテクション処理手段とを具備し、

前記代理構成手段は、前記第1のネットワーク上の装置と前記第2のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第1のコピープロテクション処理手段を用いて該第1のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第2のコピープロテクション処理手段を用いて前記第2のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする中継装置。

#### 【請求項5】

前記第2のコピープロテクション処理手段による前記所定のコンテンツ保護手続きの相手は、前記代理構成手段が代理サービスを提供している前記第2のネットワーク上の装置またはサービスまたはサブユニットであることを特徴とする請求項4に記載の中継装置。

#### 【請求項6】

前記第1のインタフェース手段または前記第2のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第1のインタフェース手段または前記第2のインタフェース手段の一方か

ら受信された前記暗号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第1のインタフェース手段または前記第2のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備したことを特徴とする請求項4に記載の中継装置。

【請求項7】

少なくとも前記復号化手段および前記暗号化手段は同一のLSIに封止されていることを特徴とする請求項6に記載の中継装置。

【請求項8】

前記特定のコンテンツは前記所定のコンテンツ保護手続きにて保護されるコンテンツであることを特徴とする請求項3または6に記載の中継装置。

【請求項9】

前記第2のネットワーク上の装置またはサービスまたはサブユニットを構成認識する構成認識手段をさらに具備したことを特徴とする請求項2または4に記載の中継装置。

【請求項10】

前記代理構成手段は、さらに、前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第3の情報を、代理で受信し、前記第1のネットワーク上の装置またはサービスまたはサブユニットへの第4の情報に変換して、送信することを特徴とする請求項2または4に記載の中継装置。

【請求項11】

前記代理構成手段は、前記第1のネットワークの装置に対してデータを送信する際に、あらかじめ該第1のネットワークの装置に対して自中継装置が代理構成

している該データを送信する装置またはサービスまたはサブユニットを通知することを特徴とする請求項 2 または 4 に記載の中継装置。

【請求項 1 2】

第 1 のネットワークに接続された第 1 のインタフェース手段と、

前記第 1 のネットワークに接続された所定の中継装置を介して通信可能な第 2 のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行うコピープロテクション処理手段とを具備したことを特徴とする通信装置。

【請求項 1 3】

前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、

このパケット送受信手段は、前記中継装置が、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この代行サービスを通して該第 2 のネットワーク上の装置またはサービスまたはサブユニットとの間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うことを特徴とする請求項 1 2 に記載の通信装置。

【請求項 1 4】

前記コピープロテクション処理手段は、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットの持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つことを特徴とする請求項 1 3 に記載の通信装置。

【請求項 1 5】

前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、

このパケット送受信手段は、前記中継装置が、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この中継装置との間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うことを特徴とする請求項 1 2 に記載の通信装置。

【請求項 1 6】

前記コピープロテクション処理手段は、前記中継装置の持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つことを特徴とする請求項 15 に記載の通信装置。

【請求項 17】

前記中継装置に対して、前記コピープロテクション処理手段が認証フォーマットを持つことを示す情報を含む自通信装置の構成情報を送信する送信手段をさらに具備したことを特徴とする請求項 12 に記載の通信装置。

【請求項 18】

第 1 のネットワークに接続された第 1 のインタフェース手段と、  
第 2 のネットワークに接続された第 2 のインタフェース手段と、  
第 1 のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第 1 のコピープロテクション処理手段と、

第 2 のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第 2 のコピープロテクション処理手段と、

前記第 1 のインタフェース手段または前記第 2 のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、

前記第 1 のインタフェース手段または前記第 2 のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第 1 のコピープロテクション処理手段または前記第 2 のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、

前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、

前記復号化されたデータを、前記第 1 のコピープロテクション処理手段または前記第 2 のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、

前記暗号化されたデータを、前記第 1 のインタフェース手段または前記第 2 のインタフェース手段の他方へ転送するコンテンツ送信手段とを具備したことを特徴とする中継装置。

## 【請求項 19】

前記第 2 のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第 1 のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第 1 の情報を、代理で受信し、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットへの第 2 の情報に変換して、送信するとともに、前記第 1 のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第 2 のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第 3 の情報を、代理で受信し、前記第 1 のネットワーク上の装置またはサービスまたはサブユニットへの第 4 の情報に変換して、送信する代理構成手段をさらに具備し、

前記代理構成手段は、前記第 1 および第 2 のネットワークの一方のネットワーク上の装置と前記第 1 および第 2 のネットワークの他方のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第 1 のコピープロテクション処理手段または前記第 2 のコピープロテクション処理手段の該当する一方を用いて該一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記他方のネットワーク上の装置またはサービスまたはサブユニットと、前記第 1 のコピープロテクション処理手段または前記第 2 のコピープロテクション処理手段の該当する他方を用いて、該所定のコンテンツ保護手続きを行うことを特徴とする請求項 18 に記載の中継装置。

## 【請求項 20】

前記コンテンツ受信手段は、前記第 2 のコピープロテクション処理手段を用いて、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第 1 のコピープロテクション処理手段を用いて、前記第 1 のネットワーク上の装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うことを特徴とする請求項 18 に記載の中継装置。

## 【請求項 21】

第1の装置の制御に供される画面描画のためのプログラムを含む、第1の制御プログラムを受信し、これを稼働するプロセッサ手段と、

このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、

前記パネル画面へのコマンドと、前記第1の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と、

前記パネル画面をサブユニットとして第2の装置に公開するサブユニット処理手段と、

前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第1の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする通信装置。

#### 【発明の詳細な説明】

##### 【0001】

#### 【発明の属する技術分野】

本発明は、IEEE 1394バスや無線ネットワーク等のネットワーク間のデータ転送を中継する中継装置及び無線ネットワーク等のネットワークを介して通信を行う通信装置に関する。

##### 【0002】

#### 【従来の技術】

近年、デジタル放送の開始や、デジタルAV機器の発売等、いわゆる「家庭AV環境のデジタル化」が大きな注目を集めている。デジタルAVデータは、様々な圧縮が可能、マルチメディアデータとしても処理が可能、何回再生しても劣化がない、等の優れた特徴を持ち、今後その用途はますます広がっていくものと考えられる。

##### 【0003】

しかしながら、このデジタルAV技術には、反面、「コンテンツの不正コピーが容易に行える」という側面もある。すなわち、どのようなデジタルコンテンツについても、原理的に「ビットのコピー」で、元どおりの品質の、しかも未来永劫にわたって一切劣化のない複製が作れてしまうため、いわゆる「不正コピー」

の問題が発生する。

【0004】

この「不正コピー」を防ぐための技術がいくつか検討されている。その中の一つが、CPTWG（コピープロテクション技術ワーキンググループ）で検討されている「1394CPコンテンツ保護システム仕様（1394CP Content Protection System Specification）」である。この技術は、IEEE1394バスに接続されたノード間で、転送するコンテンツ（例えばMPEGデータ等）について、送受信ノードの間で予め認証手続きを行い、暗号鍵（コンテンツキー）を共有できるようにしておき、以降は転送するコンテンツを暗号化して転送し、認証手続きを行った両者以外はコンテンツが読めないようにする技術である。このようにすることにより、認証手続きを行っていないノードは、コンテンツキーの値がわからないため、転送されているデータ（暗号化されているデータ）をたとえ取り込むことができたとしても、この暗号を復号化することはできない。このような認証に参加できるノードは、あらかじめ定められた認証機関が許可したノードのみとしておくことで、不正なノードが暗号鍵を入手することを未然に防ぎ、不正コピーを予め防ぐことが可能になる。

【0005】

【発明が解決しようとする課題】

IEEE1394バスは、最低速度でも100Mbps、網そのものに自動構成認識機能が備わっている、QOS転送機能を持つ等、非常に優れた特徴を持つネットワークシステムであり、それゆえに家庭向けのデジタルAV向けのネットワークとして、デファクトスタンダードの地位を築いている。

【0006】

しかし、IEEE1394は、これら特徴のゆえに、「IEEE1394と、他のネットワークを接続するとき」に様々な制約を生んでいる。例えば、無線網や公衆網とIEEE1394バスを接続する場合は、これらの網が100Mbps以上といった高速性を一般には有していないことや、IEEE1394の自動構成認識機能をこれらの網へそのまま拡張する、といった方法が簡単にはとれな

いことから、IEEE 1394 プロトコルをそのまま無線や公衆網に拡張する、といった方法を使うことはできない。そこで、IEEE 1394 と、無線網や公衆網などの他網の間にプロトコル変換ゲートウェイを配置し、相互接続する方法や、片方の網上のサービスをもう片方の網のサービスとして提供するいわゆる代理サーバの方法等が提案されている。

【0007】

これらの方法を、従来の技術で述べた 1394 コピープロテクションに適用しようとした場合、現状では該コピープロテクション技術が IEEE 1394 バスについてのみ定められている状況である。このコピープロテクション技術を「IEEE 1394 と、他のネットワークを接続するとき」に拡張するための技術はないのが現状である。

【0008】

本発明は、上記事情を考慮してなされたもので、コピープロテクション技術を IEEE 1394 のみならず、これと相互接続された他網にも拡張可能な中継装置及び通信装置を提供することを目的とする。

【0009】

また、本発明は、同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置及び通信装置を提供することを目的とする。

【0010】

【課題を解決するための手段】

本発明（請求項 1）に係る中継装置は、第 1 のネットワークに接続された第 1 のインタフェース手段と、第 2 のネットワークに接続された第 2 のインタフェース手段と、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第 1 のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第 1 の情報を、代理で受信し、前記第 2 のネットワーク上の装置またはサービスまたはサブユニットへの第 2 の情報に変換して、送信する代理構成手段と、前記第 1 のネットワーク上の装置からの前記第 1 の情報を受信した際、この情報が少なくとも所定の情報であるか否かを検出する検出手段と、前記検出手段により、検出した第 1 の情報が前記所定の情報で

あった場合には、前記所定の情報を前記第2のネットワーク上の装置またはサービスまたはサブユニットに転送する転送手段とを具備したことを特徴とする。

## 【0011】

好ましくは、本発明（請求項2）のように、請求項1に記載の中継装置において、前記所定の情報は、前記第1のネットワーク上の装置と前記第2のネットワーク上の装置またはサービスまたはサブユニット間で送受信される情報を保護するための情報であり、少なくとも認証手続きに関する情報からなるものであるようにしてもよい。

## 【0012】

本発明（請求項2）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第2のネットワーク上の装置またはサービスまたはサブユニット（以下、装置またはサービスまたはサブユニットを装置等と呼ぶ）」と「第1のネットワーク上の装置」との間において、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がその手続きを中身を変えることなく中継することによって、そのコンテンツ保護手続きを直接「代理構成手段が提供している第2のネットワーク上の装置等」と「第1のネットワーク上の装置」との間において行うことができる。

## 【0013】

なお、少なくとも認証手続きを含むコンテンツ保護手続きは、例えば、認証手続き、認証手続きおよび鍵交換手続き、などである。

## 【0014】

好ましくは、本発明（請求項3）のように、請求項2に記載の中継装置において、前記第1のインタフェース手段または前記第2のインタフェース手段から特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第1のイン

タフェース手段または前記第2のインタフェース手段の一方から受信された前記特定のコンテンツを含むデータを、前記第1のインタフェース手段または前記第2のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備するようにしてもよい。

## 【0015】

本発明（請求項3）によれば、保護されるべきコンテンツを、その保護形式を変更することなく受信側に送り届けることができ、請求項2にて処理されるコンテンツ保護形式にて、そのコンテンツを保護された形でエンドエンドに送り届けることができる。

## 【0016】

本発明（請求項4）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、前記第2のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第1の情報を、代理で受信し、前記第2のネットワーク上の装置またはサービスまたはサブユニットへの第2の情報に変換して、送信する代理構成手段と、前記第1のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第1のコピープロテクション処理手段と、前記第2のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第2のコピープロテクション処理手段とを具備し、前記代理構成手段は、前記第1のネットワーク上の装置と前記第2のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第1のコピープロテクション処理手段を用いて該第1のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記第2のコピープロテクション処理手段を用いて前記第2のネットワーク上の装置またはサービスまたはサブユニットと該所定のコンテンツ保護手続きを行うことを特徴とする。

## 【0017】

本発明（請求項4）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「第2のネットワーク上の装置等」と「第1のネットワーク上の装置」との間において、「第1のネットワーク上の装置」または「第2のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第1のネットワーク上の装置」または「第2のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「第2のネットワーク上の装置等」と中継装置との間、および中継装置と「第1のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

## 【0018】

好ましくは、本発明（請求項5）のように、請求項4に記載の中継装置において、前記第2のコピープロテクション処理手段による前記所定のコンテンツ保護手続きの相手は、前記代理構成手段が代理サービスを提供している前記第2のネットワーク上の装置またはサービスまたはサブユニットであるようにしてもよい。

本発明（請求項5）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「代理構成手段が提供している第2のネットワーク上の装置等」と「第1のネットワーク上の装置」との間において、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「第1のネットワーク上の装置」または「代理構成手段が提供している第2のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、中継装置が、コンテンツ保護手続きをそれぞれ終端することで、結局、「代理構成手段が提供している第2のネットワーク上の装置等」と中継装置との間、および中継装置と「第1のネットワーク上の装置」との間で、コンテンツ保護手続きをそれぞれ行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

【0019】

好ましくは、本発明（請求項6）のように、請求項4に記載の中継装置において、前記第1のインタフェース手段または前記第2のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第1のインタフェース手段または前記第2のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第1のインタフェース手段または前記第2のインタフェース手段の他方へ転送するコンテンツ送信手段とをさらに具備するようにしてもよい。

【0020】

本発明（請求項6）によれば、第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、不正コピー等を未然に防ぐことが可能になる。

【0021】

好ましくは、本発明（請求項7）のように、請求項6に記載の中継装置において、少なくとも前記復号化手段および前記暗号化手段は同一のLSIに封止されているようにしてもよい。

【0022】

本発明（請求項7）によれば、この復号化手段と暗号化手段との間は、暗号化されていないコンテンツデータが流れるため、個々にプローブをあてる等して、ここからコンテンツデータを盗聴し、不正コピーを働くことを未然に防止することが可能となる。

【0023】

好ましくは、本発明（請求項8）のように、請求項3または6に記載の中継装置において、前記特定のコンテンツは前記所定のコンテンツ保護手続きにて保護

されるコンテンツであるようにしてもよい。

【0024】

本発明（請求項8）によれば、保護されるべきコンテンツをエンドエンドに転送することができる。

【0025】

好ましくは、本発明（請求項9）のように、請求項2または4に記載の中継装置において、前記第2のネットワーク上の装置またはサービスまたはサブユニットを構成認識する構成認識手段をさらに具備するようにしてもよい。

【0026】

本発明（請求項9）によれば、代理構成手段が構成する代理サービスを、自動的に構成することができるようになり、もって、コンテンツ保護手続きに至る手順のプラグアンドプレイでの実現が可能になる。

【0027】

好ましくは、本発明（請求項10）のように、請求項2または4に記載の中継装置において、前記代理構成手段は、さらに、前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第3の情報を、代理で受信し、前記第1のネットワーク上の装置またはサービスまたはサブユニットへの第4の情報に変換して、送信するようにしてもよい。

【0028】

本発明（請求項10）によれば、コンテンツ保護手続きとして、第2のネットワーク上の装置等から、第1のネットワーク上の装置等への方向の手続きが必要な場合に、当該中継装置がその仲立ちを行うことができる。

【0029】

好ましくは、本発明（請求項11）のように、請求項2または4に記載の中継装置において、前記代理構成手段は、前記第1のネットワークの装置に対してデータを送信する際に、あらかじめ該第1のネットワークの装置に対して自中継装置が代理構成している該データを送信する装置またはサービスまたはサブユニットを通知するようにしてもよい。

【0030】

本発明（請求項11）によれば、この通知を受信した第1のネットワーク上の装置に対して、どこに認証要求を出せばよいかを通知することが可能になる。

【0031】

本発明（請求項12）に係る通信装置は、第1のネットワークに接続された第1のインタフェース手段と、前記第1のネットワークに接続された所定の中継装置を介して通信可能な第2のネットワーク上の装置またはサービスまたはサブユニットとの間で、少なくとも認証手続を含む所定のコンテンツ保護手続を行うコピープロテクション処理手段とを具備したことを特徴とする。

【0032】

本発明（請求項12）によれば、直接第1のネットワークで接続されていない装置等との間で、コンテンツ保護手続を行うことができるようになる。

【0033】

好ましくは、本発明（請求項13）のように、請求項12に記載の通信装置において、前記所定のコンテンツ保護手続に関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、このパケット送受信手段は、前記中継装置が、前記第2のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この代行サービスを通して該第2のネットワーク上の装置またはサービスまたはサブユニットとの間で前記所定のコンテンツ保護手続に関する情報を含むパケットのやり取りを行うようにしてもよい。

本発明（請求項13）によれば、第2のネットワーク上の装置等と直接の通信機能を持っていない場合においても、パケットの送受信先を中継装置の代理サービスとし、この代理サービスを通して、第2のネットワーク上の装置等と、コンテンツ保護手続を行うことができるようになる。

【0034】

好ましくは、本発明（請求項14）のように、請求項13に記載の通信装置において、前記コピープロテクション処理手段は、前記第2のネットワーク上の装置またはサービスまたはサブユニットの持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つようにしてもよい。

【0035】

本発明（請求項14）によれば、同一の認証機関が定めたコンテンツ保護手続きを、自通信装置と第2のネットワーク上の装置等とのエンドエンド間で行うことができる。

【0036】

好ましくは、本発明（請求項15）のように、請求項12に記載の通信装置において、前記所定のコンテンツ保護手続きに関する情報を含むパケットを送受信するパケット送受信手段をさらに具備し、このパケット送受信手段は、前記中継装置が、前記第2のネットワーク上の装置またはサービスまたはサブユニットの代行サービスを提供している場合に、この中継装置との間で前記所定のコンテンツ保護手続きに関する情報を含むパケットのやり取りを行うようにしてもよい。

本発明（請求項15）によれば、第2のネットワーク上の装置等との直接の通信機能を持っていない場合においても、パケットの送受信先を中継装置の代理サービスとし、自通信装置と中継装置との間でコンテンツ保護手続きを行い、第2のネットワーク上の装置等と中継装置との間のコンテンツ保護手続きについては、中継装置にまかせることで、結局、エンドエンドのコンテンツ保護手続きを行うことができる。

【0037】

好ましくは、本発明（請求項16）のように、請求項15に記載の通信装置において、前記コピープロテクション処理手段は、前記中継装置の持つ認証フォーマットの発行機関と同じ発行機関により発行された認証フォーマットを持つようにしてもよい。

【0038】

本発明（請求項16）によれば、同一の認証機関が定めたコンテンツ保護手続きを、自通信装置と中継装置とのエンドエンド間で行うことができる。

【0039】

好ましくは、本発明（請求項17）のように、請求項12に記載の通信装置において、前記中継装置に対して、前記コピープロテクション処理手段が認証フォーマットを持つことを示す情報を含む自通信装置の構成情報を送信する送信手段

をさらに具備するようにしてもよい。

【0040】

本発明（請求項17）によれば、中継装置に対して、自通信装置に暗号化データを送信することが可能であることを通知することができる。また、中継装置がこの通知を第2のネットワーク上に開示等することで、第2のネットワーク上の装置は、その旨を知ることができる。

【0041】

本発明（請求項18）に係る中継装置は、第1のネットワークに接続された第1のインタフェース手段と、第2のネットワークに接続された第2のインタフェース手段と、第1のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第1のコピープロテクション処理手段と、第2のネットワーク上の装置またはサービスまたはサブユニットと、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う第2のコピープロテクション処理手段と、前記第1のインタフェース手段または前記第2のインタフェース手段から暗号化された特定のコンテンツを含むデータを受信するコンテンツ受信手段と、前記第1のインタフェース手段または前記第2のインタフェース手段の一方から受信された前記暗号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する一方で提供されるコンテンツ保護用の鍵で復号化する復号化手段と、前記復号化されたデータを、別の符号化形式のデータに変換する変換手段と、前記復号化されたデータを、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する他方で提供されるコンテンツ保護用の鍵で暗号化する暗号化手段と、前記暗号化されたデータを、前記第1のインタフェース手段または前記第2のインタフェース手段の他方へ転送するコンテンツ送信手段とを具備したことを特徴とする。

【0042】

本発明（請求項18）によれば、第1のネットワークを伝送させるデータが保護されるべきコンテンツであり、且つ、第1のネットワークと第2のネットワークの通信帯域が著しく異なる場合のように、第2のネットワークに元のデータと

は異なるデータ形式で転送することが求められた場合に、変換手段によってデータ形式の変換を行いつつ、第1のネットワーク上の装置から第2のネットワーク上の装置等の間の全ての経路において、転送されるデータは暗号化されていることになり、両区間（両データ形式）においても、不正コピー等を未然に防ぐことが可能になる。

## 【0043】

好ましくは、本発明（請求項19）のように、請求項18に記載の中継装置において、前記第2のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第1のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第1の情報を、代理で受信し、前記第2のネットワーク上の装置またはサービスまたはサブユニットへの第2の情報に変換して、送信するとともに、前記第1のネットワーク上の装置またはサービスまたはサブユニットを、自中継装置上のものとして、前記第2のネットワーク側に開示し、この装置またはサービスまたはサブユニット宛の第3の情報を、代理で受信し、前記第1のネットワーク上の装置またはサービスまたはサブユニットへの第4の情報に変換して、送信する代理構成手段をさらに具備し、前記代理構成手段は、前記第1および第2のネットワークの一方のネットワーク上の装置と前記第1および第2のネットワークの他方のネットワーク上の装置またはサービスまたはサブユニットへの、少なくとも認証手続きを含む所定のコンテンツ保護手続きを行う場合には、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する一方を用いて該一方のネットワーク上の装置と該所定のコンテンツ保護手続きを行うとともに、前記他方のネットワーク上の装置またはサービスまたはサブユニットと、前記第1のコピープロテクション処理手段または前記第2のコピープロテクション処理手段の該当する他方を用いて、該所定のコンテンツ保護手続きを行うようにしてもよい。

## 【0044】

本発明（請求項19）によれば、保護すべきコンテンツの送信もしくは受信を行っているペアである「他方のネットワーク上の装置等」と「一方のネットワーク上の装置」との間において、「一方のネットワーク上の装置」または「他方の

ネットワーク上の装置等」が、あくまでコンテンツ保護手続きの相手は当該中継装置であると認識しつつ、コンテンツ保護手続きを行うことができるため、「一方のネットワーク上の装置」または「他方のネットワーク上の装置等」は、中継装置を経て接続される別のネットワークについて考慮をする必要がなくなる。また、実際には、中継装置がそのコンテンツ保護手続きをそれぞれ終端することで、結局、「他方のネットワーク上の装置等」と中継装置、および中継装置と「一方のネットワーク上の装置」との間に、コンテンツ保護手続きを行うこととなり、結局、エンドエンドでコンテンツの保護を行うことができる。

## 【0045】

好ましくは、本発明（請求項20）のように、請求項18に記載の中継装置において、前記コンテンツ受信手段は、前記第2のコピープロテクション処理手段を用いて、前記第2のネットワーク上の装置またはサービスまたはサブユニットと、前記所定のコンテンツ保護手続きのうち少なくとも一部を行ってそれが正常に終了した場合に、前記第1のコピープロテクション処理手段を用いて、前記第1のネットワーク上の装置またはサービスまたはサブユニットと前記所定のコンテンツ保護手続きのうち少なくとも一部を行うようにしてもよい。なお、前記所定のコンテンツ保護手続きのうち少なくとも一部は、例えば、認証手続きである。

本発明（請求項20）によれば、第2のネットワーク上の装置またはサービスまたはサブユニットが信頼に足るデバイスであるかどうかを未然に知ることができるようになり、まず第2のネットワーク上の装置等と認証手続きを行い、その後、第1のネットワーク上の装置等との認証に失敗した場合に、第1のネットワーク上の装置等との認証を改めて行わなくてもよい分、通信資源や処理資源の節約になる。

## 【0046】

本発明（請求項21）に係る通信装置は、第1の装置の制御に供される画面描画のためのプログラムを含む、第1の制御プログラムを受信し、これを稼働するプロセッサ手段と、このプロセッサ手段が描画する画面のうちの少なくとも一部を構成するパネル画面を作成する画面作成手段と、前記パネル画面へのコマンドと、前記第1の装置の制御のためのコマンドとの対応関係を記憶する記憶手段と

、前記パネル画面をサブユニットとして第2の装置に公開するサブユニット処理手段と、前記サブユニットへのコマンドを受信した場合、前記記憶手段を参照してこのコマンドを前記第1の装置の制御のためのコマンドに変換して、これを送出する手段とを具備したことを特徴とする。

【0047】

一般に、前記のような制御プログラムを稼働させるためには、仮想マシンと呼ばれ計算環境を用意する必要があるのに対し、パネル画面を通した機器制御は、簡単なコマンド体型を用意するだけでよいため、簡単な計算環境を用意しておけばよい。本発明（請求項21）によれば、前記制御プログラムを持たない第2の装置に対しても、パネル画面という形で、前記第1の装置の制御インタフェースを提供することが可能になる。

【0048】

なお、装置に係る本発明は方法に係る発明としても成立し、方法に係る本発明は装置に係る発明としても成立する。

【0049】

また、装置または方法に係る本発明は、コンピュータに当該発明に相当する手順を実行させるための（あるいはコンピュータを当該発明に相当する手段として機能させるための、あるいはコンピュータに当該発明に相当する機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても成立する。

【0050】

#### 【発明の実施の形態】

以下、図面を参照しながら発明の実施の形態を説明する。

【0051】

#### （第1の実施形態）

図1は、ある家庭のホームネットワークの全体構成の一例である。

【0052】

このホームネットワークには、送信ノード101、中継ノード102、無線ノード103の3つが接続されており、送信ノード101と中継ノード102は（

有線の) IEEE 1394 バス 104 に、中継ノード 102 と無線ノード 103 は無線網にそれぞれ接続されている。ただし、後述するような方法で、各々のノードは互いに通信ができるようになっている。

#### 【0053】

本実施形態では、送信ノード 101 から送出された MPEG 映像を、中継ノード 102 で中継し、無線区間を経由して無線ノード 103 に送信する場合を例として説明する。その際に、著作権保護（不正コピーの防止）のために、送信ノード 101 と無線ノード 103 との間で転送される MPEG 映像データは暗号化される場合を考える。

#### 【0054】

なお、図 1 では、3 つのノードを示してあるが、もちろん、これらの他にノードが接続されていてもよい（後述する他の実施形態においても同様である）。

#### 【0055】

図 2 に、送信ノード 101 の内部構造の一例を示す。

#### 【0056】

送信ノード 101 は、内部に MPEG 映像データを蓄積している装置であり、要求に応じて MPEG 映像データを IEEE 1394 バス 104 を通じて送出する。その際、IEEE 1394 バス上において不法コピーをされることを未然に防止するために、必要な場合には送出する MPEG 映像データを暗号化して送出する機能を持つ。そのため、MPEG 映像データを受信するノードと、認証データ、暗号鍵等の交換を行うための機構も持つ。

#### 【0057】

図 2 に示されるように、この送信ノード 101 は、IEEE 1394 インタフェース 401、AV/C プロトコルの処理を行う AV/C プロトコル処理部 402、AV/C プロトコル内のコピープロテクションに関する処理を行うコピープロテクション処理部 403、IEEE 1394 を通して送受信されるデータのうち、同期チャンネルを通してやり取りされるデータについて送受信する ISO 信号送受信部 404、MPEG 映像のストレージである MPEG ストレージ部 406、コピープロテクション処理部 403 から暗号鍵 K をもらい、MPEG 映像を暗

号化して I S O 信号送受信部 404 に送出する暗号化部 405 を有する。ここで、コピープロテクション処理部 403 は、認証のためのフォーマット A c e r t を持つ。

#### 【0058】

次に、図 3 に、中継ノード 102 の内部構造の一例を示す。

#### 【0059】

中継ノード 102 は、I E E E 1394 バス側から受信したデータ (M P E G 映像データ) を無線区間側にフォワードする機能の他に、I E E E 1394 バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対して I E E E 1394 バス側のノード (本実施形態では送信ノード 101) の代理サーバとなり、I E E E 1394 バス側のノードの機能を代理で提供する機能が存在する。

#### 【0060】

図 3 に示されるように、この中継ノード 102 は、I E E E 1394 インタフェース 201、無線インタフェース 202、A V / C プロトコル処理部 203、I S O 信号送受信部 204、無線区間側の同期チャネルの信号の送受信を行う無線 I S O 信号送受信部 205、I E E E 1394 バス上のノードの構成情報を収集したり、自らの構成情報 (自分がどのような機能を持っているかについての情報等) を I E E E 1394 上に広告する機能を持つ 1394 バス構成認識部 206、I E E E 1394 バス側に対して無線区間側のノードやサービス (サブユニット) を代理で公開したり、無線区間側のノードやサービスへのコマンド等を代理で受け付け、これを無線区間側に必要に応じてプロトコル変換をして送出したり、あるいは無線区間側に対して I E E E 1394 側のノード / サービス (サブユニット) の代理公開やコマンドの代理受付 / 翻訳等を行う代理サブユニット構成部 207、無線区間上のノードの構成情報を収集したり、自らの構成情報 (自分がどのような機能を持っているかについての情報等) を無線区間上に広告する機能を持つ無線区間構成認識部 209、コピープロテクションに関する処理を行い、1394 バスと無線区間をまたがるコピープロテクション処理に関しては、やり取りされる情報を透過的にフォワードさせるコピープロテクション制御 / フ

ワード部 210、無線区間でやり取りされる制御パケットの送受信を行う無線ノード制御パケット送受信部 211 を有する。

【0061】

次に、図 4 に、無線ノード 103 の内部構造の一例を示す。

【0062】

無線区間においていわゆる IEEE 1394 プロトコル（物理レイヤプロトコル、リンクレイヤプロトコル等）が稼働している必要は必ずしもなく、IEEE 802.11 や無線 LAN 等、任意の無線プロトコルを利用することを想定するが、本実施形態では、特に、いわゆる QOS 機能（同期通信機能）を持つ無線網であることを仮定する。ただし、本実施形態は、無線区間部分に QOS 機能が求められると制限されるものではない。

【0063】

いわゆる IEEE 1394 ノードではない無線ノード 103 が、IEEE 1394 バスにつながれたノード（本実施形態では送信ノード 101）と通信を行うために、前述のように、中継ノード 102 が IEEE 1394 バス上のノードや機能（サブユニット）をエミュレートしている。すなわち、無線ノード 103 から見て、中継ノード 102 はいわゆる IEEE 1394 バス側のノードや機能の代理サーバとなっている。無線ノード 103 は、これら（IEEE 1394 側のノードや機能）を中継ノード 102 の機能と考え、通信を行うが、実際には中継ノード 102 が必要なプロトコル変換やデータの乗せ換えを行う。

【0064】

図 4 に示されるように、この無線ノード 103 は、無線インタフェース 301、無線ノード制御パケット送受信部 302、コピープロテクション処理部 303、無線 ISO 信号送受信部 304、受信した暗号化されたストリーム（MPEG 映像等）を、コピープロテクション処理部 303 から渡されるコンテンツキー K を使ってこれを復号化する暗号復号化部 305、MPEG デコード部 306、映像を表示するディスプレイ部 307 を有する。

【0065】

無線ノード 103 のコピープロテクション処理部 303 は、後述するように、

認証フォーマットBcertを持ち、その認証の発行機関は、送信ノード101（の映像送出サブユニット）の認証フォーマットAcertの発行機関と同一の発行機関である。

#### 【0066】

次に、実際のコピープロテクションを施した上でのMPEG映像全体のシーケンスについて、図5／図6（全体のシーケンス例）、図7／図8（送信ノード101のフローチャート例）、図9／図10／図11（中継ノード102のフローチャート例）、図12／図13（無線ノード103のフローチャート例）を参照しながら説明する。

#### 【0067】

まず、無線ノード103は、自分の構成情報を中継ノード102に通知する（ステップS501）。この通知は、無線ノード内にIEEE1212レジスタを用意し、ここに自分の構成情報を記しておく形で行われてもよい。構成情報とは、自分（無線ノード）がMPEGデコード／ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、などである。ここで、この認証フォーマットが、特定のコピープロテクション機関が定めたフォーマットであることを同時に通知したり、IEEE1394向けのコピープロテクションのための認証フォーマットである旨を同時に通知してもよい。

#### 【0068】

ここで、認証について簡単に説明する。

#### 【0069】

ネットワーク上を映画やテレビ番組などの著作権を考慮すべきコンテンツ（データ）を転送する場合、それらのコンテンツは暗号によって保護を行うべきである。なぜなら、これらのデータの転送中に、ネットワーク上で盗聴された場合、不正コピーが可能となってしまうからである。これに対する対策としては、転送するデータの暗号化が有効である。

#### 【0070】

次に問題となるのが、「怪しいものにデータを送っている危険はないか」という問題である。たとえ、データを暗号化して送ったとしても、送った先のノード

（暗号を解く鍵を持っている）が悪意を持っている場合（不正コピーをしようと考えている場合）には、やはり解読可能な形でデータを送るべきではない。これに対する対策が認証である。すなわち、この暗号を解く鍵を受信側に渡す前に、受信側が不正を働かないものかどうかの確認をとる（確認が取れた受信側ノードにのみ暗号を解く鍵を渡す）仕組みである。

## 【0071】

具体的には、予め認証機関が「このノード（あるいはサブユニット）は、不正に働くことはない」と認定したノード（あるいはサブユニット）に対して、「認証フォーマット」と呼ばれるデータを、あらかじめ送信側のノードと受信側のノードとの両方に与えておく。この「認証フォーマット」を正しい形で持っているということは、そのノード（あるいはサブユニット）は信用できる（不正を働かない）と考えることができる。そこで、上記のデータ転送に先立って、送受信ノード（あるいはサブユニット）間で認証フォーマットのやり取りを行い、正しい形で認証フォーマットが確認できた場合に限り、暗号を解くための鍵（もしくは鍵を生成するための元となるデータ）を通知し、その鍵で暗号化されたデータをネットワーク上を転送する、という手法をとる。

## 【0072】

さて、無線ノード103は、このような認証フォーマットをあらかじめ認証機関により与えられており、「暗号化データを正当な形で受信／再生する権利」を持っている。ここで、無線ノード103が持っている認証フォーマットを「B c e r t」とする。

## 【0073】

無線ノード103は、図5のステップS501で自分の構成情報を通知する際に、自分は認証フォーマットを有していることを、この構成情報に加えてもよい（ステップS801）。例えば、図14のように、構成情報の中に、本無線ノード103がMPEGデコード／ディスプレイ機能を持っており、さらに該機能が認証フォーマットを持っていること、その認証フォーマットがどの発行機関が発行したものか、等の情報を有する。

## 【0074】

なお、中継ノード102が無線ノード103の構成を認識する方法としては、この他にも中継ノード102が無線ノード103に対して構成を問い合わせるパケットを送信し、無線ノード103がこれに答える方法等も可能である。

【0075】

さて、この構成情報を受信した中継ノード102は、無線ノード103が認証フォーマットを持つことや、MPEGデコード／ディスプレイ機能を持っていることを確認する（ステップS701）。

【0076】

中継ノード102は、無線ノード103がMPEGデコード／ディスプレイ機能を持っていることをIEEE1394バス側のノードに対して知らせるため、このMPEGデコード／ディスプレイ機能を、中継ノード102自身のサブユニットとしてIEEE1394バス側に広告する（ステップS502）。具体的には、IEEE1212レジスタに「自分はMPEGデコード／ディスプレイ機能を持っている」旨を記載したり、AV／Cプロトコルでサブユニット構成の問い合わせを受けた場合に、自分がMPEGデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、IEEE1394に接続されたノードは、中継ノード102にこの機能が存在すると認識することになる）。

【0077】

そのために、中継ノード102は、代理サブユニット構成部207内に代理テーブル208を持つ。代理テーブル208は、図15／図16のように、中継ノード102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0078】

ここでは、図15のように、無線ノード103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS702，S703）。

【0079】

このため、送信ノード101から見た中継ノード102の構造は図17のよう

に見えることになる（ステップS601）。

【0080】

以上は、IEEE1394バス側についての説明であったが、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード102は、IEEE1394バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図16のような設定がなされ、無線ノードから見た中継ノード102の構造は図18のように見える。

【0081】

さて、中継ノード102内にMPEGデコード／ディスプレイサブユニットがあると認識した送信ノード101は、このサブユニットに対して、MPEG映像を転送することを目的に、1394バス上に同期チャンネル#xを確立し、AV／Cプロトコルにて「この同期チャンネル#x（を受信するプラグ）と、MPEGデコード／ディスプレイサブユニットとを接続し、映像を表示せよ」との命令をだす（ステップS503，S602）。送信ノード101は、このサブユニットが中継ノード101にあたるものと解釈しているため、命令の送信先は中継ノード102である。

【0082】

これを受信（ステップS704）した中継ノード102は、受信した命令パッケージを解釈し、その命令が自らが代理サービスを行っているMPEGデコード／ディスプレイサブユニットに対する命令であることを認識し、代理テーブル208を参照して、この命令先の実体は無線ノード103にあることを認識する（ステップS705）。

【0083】

よって、IEEE1394バスの同期チャンネル#xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャンネル（#y）の確保を行い（ステップS706）、さらにISO信号送受信部204（同期チャンネル#xを受信）と無線ISO信号送受信部205（同期チャンネル#yを送信）を接続し、1394インタフェース201から入力された入力データ（ISOデータ）を無線区間にフォワードできるようにする（ステップS504，S707）。

【0084】

さらに、無線ノード103に対して、「無線同期チャンネル#yを通してデータを送信するので、これを受信し、MPEGデコーダに入力し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形で送信する（ステップS505, S708）。

【0085】

図19に、この無線ノード制御パケットの一例を示す。

【0086】

図19に示されるように、無線ノード103に無線同期チャンネル#yを通して送信したデータ（MPEG映像）を、MPEGデコード／ディスプレイ機能に転送し、表示することを促す内容となっている。また、この中にこのデータ（MPEG映像）を送信するサブユニット（中継ノード102の映像送信機能；実際には、送信ノード101の代理でその機能を持っていると広告している）についての情報も併せて通知している。

【0087】

これを受信した無線ノード103は、無線同期チャンネル#yを通してデータが送られてくることを認識する（ステップS802）。無線ノード103は、このデータの送信元は中継ノード102の映像送信サブユニットであると認識する（前述のように、実際のデータ送信元は送信ノード101である）。このため、この無線ノード制御パケット内に、「この無線同期チャンネルを通して送信されるデータの送信元は中継ノード102の映像送信サブユニットである」との情報を含めてもよい。

【0088】

この後、送信ノード101は、同期チャンネル#xを通して、暗号化されたMPEG映像を転送する（ステップS603, S506）。これを受信した中継ノード102は、先に設定したようにこれを無線区間にフォワードする（ステップS709, S507）。

【0089】

このようにして、暗号化されたMPEG映像が無線ノード103に到達する（

ステップ S 8 0 3)。しかし、この時点で無線ノード 1 0 3はこの暗号を解くための鍵を有していない（もしくはその鍵を生成するための元となるデータを有していない）ため、ここから暗号を解いて、M P E G映像を取り出すことはできない。ここで、無線ノード 1 0 3は認証手続きがM P E G映像の送信元と必要であることを認識する。

【0090】

そこで、無線ノード 1 0 3（のコピープロテクション処理部 3 0 3）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード 1 0 3には、上記暗号化データの送信元は中継ノード 1 0 2（内の映像送信サブユニット）であるように認識されているので、認証要求の宛先も、中継ノード 1 0 2（内の映像送信サブユニット）である。その際、認証要求には、無線ノード 1 0 3の認証フォーマット B c e r t等を付与する（ステップ S 8 0 4， S 5 0 8）。

【0091】

これを受信（ステップ S 7 1 0）した中継ノード 1 0 2は、代理テーブル 2 0 8を参照して、この認証要求の要求先が実は送信ノード 1 0 1（の映像送信サブユニット）であることを認識し、この認証要求を、中身を変えずに（B c e r t等はそのまま残して）送信ノード 1 0 1に対してフォワードする（ステップ S 5 0 9， S 7 1 1）。

【0092】

ここで、認証要求の中身を変えずにフォワードすることで、この認証要求はそのままの形で送信ノード 1 0 1に到達することになり、結局送信ノード 1 0 1と無線ノード 1 0 3との間で、実際の認証手続きは進んでいくことになり、しかも中継ノード 1 0 2をはじめ、その他のノードにはその認証の結果明らかになる鍵の値などの情報を知られることなく、以上の手続きを行っていくことが可能である。

【0093】

これを受け取った送信ノード 1 0 1は、これを中継ノード 1 0 2のM P E Gデコード／ディスプレイサブユニットから送られてきた認証要求であると解釈する

(ステップS604)。その後、Bcertから無線ノード103のMPEGデコード/ディスプレイサブユニットを特定できるID(Bdid)を抽出し(ステップS605)、これとともに、やはり同様の認証要求を認証要求の送信元に対して行おうとする。ただし、送信ノード101は、Bcertが無線ノード103の認証フォーマットであるとは意識することではなく、むしろ中継ノード102(のMPEGデコード/ディスプレイサブユニット)の認証フォーマットであると意識をしている。

## 【0094】

この認証要求には、送信ノード101(の映像送出サブユニット)の認証フォーマットAcertと、Bdidとが含まれる。ここで、送信ノード101は、該認証要求S509の送信元は中継ノード102(のMPEGデコード/ディスプレイサブユニット)であると解釈しているため、この認証要求の送信先はやはり中継ノード102となる(ステップS606, S510)。

## 【0095】

これを受信(ステップS712)した中継ノード102は、代理テーブル208を参照して、この認証手続の本来の要求先が無線ノード103(のMPEGデコード/ディスプレイ機能)であることを認識し、この認証手続要求を、中身を変えずに(Acert等はそのまま残して)無線ノード103に対してフォワードする(ステップS511, S713)。この認証要求の送信元は中継ノード102である。

## 【0096】

これを受け取った無線ノード103は、これを中継ノード102の映像送信サブユニットから送られてきた認証要求であると解釈する(ステップS805)。その後、Acertから送信ノード101の映像サブユニットを特定できるID(Adid)を抽出し、認証鍵の交換に必要な残りの手続きを、認証要求の送信元に対して行おうとする。なお、この場合も、無線ノード103は、Acertが送信ノード101の認証フォーマットであるとは意識せず、むしろ中継ノード102(の映像送信サブユニット)の認証フォーマットであると意識する。

## 【0097】

この認証鍵の交換に必要な残りの手続きとして、無線ノード103は、認証要求の送信元（と無線ノードが解釈しているノード）に対して認証・鍵交換手続きパケットを送信する（ステップS512）。この認証・鍵交換手続きパケットには、鍵交換初期値、署名、A c e r tの中に含まれていた送信ノード（の映像送信サブユニット）のデバイスID（A d i d）等が含まれている（ステップS806）。ここで、無線ノード103は、該認証要求S511の送信元は中継ノード102（の映像送信サブユニット）であると解釈しているため、この認証要求の送信先はやはり中継ノード102となる。

## 【0098】

これを受信した中継ノード102は、代理テーブル208を参照して、この認証手続きの本来の要求先が送信ノード101（の映像送信サブユニット）であることを認識し、この認証手続きパケットを、中身を変えずに送信ノード101に対してフォワードする（ステップS513, S714）。このパケットの送信元は中継ノード102である。

## 【0099】

これと同様の手続きが送信ノード101→中継ノード102→無線ノード103の方向に対しても行われる（ステップS514, S515, S609, S715, S807）。

## 【0100】

この認証手続きパケットを受信した送信ノード101および無線ノード103は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマットが正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵K a u t hを導き出す。この共通の認証鍵K a u t hは、送信ノード（の映像送信サブユニット）と無線ノード（のMPEGデコード／ディスプレイ機能）との間で共通に持つ鍵で、この鍵K a u t hを、この両者（送信ノード101、無線ノード103）以外の他人に知られることなく共有することがこの時点で行えるようになる（ステップS608, S808）。

## 【0101】

この認証鍵`Key`を使って、実際にMPEGストリームの暗号化を行うコンテンツキー`K`の計算ができるようになる。

#### 【0102】

さて、このようにして、送信ノード101（の映像送信サブユニット）と無線ノード103（のMPEGデコード／ディスプレイ機能）との間で、コンテンツキー`K`の値が共有できるようになった。

#### 【0103】

ここで、送信ノード101が、送信するMPEG映像を、コンテンツキー`K`を使って、暗号化部405にて暗号化し（ステップS610）、これを1394バスの同期チャンネル#`x`を通して中継ノード102（のMPEGデコード／ディスプレイサブユニット）に対して送信する（ステップS516, S611）。

#### 【0104】

中継ノード102は、送信ノード101から同期チャンネル#`x`を通して送られてくる暗号化されたMPEG映像を、ISO信号送受信部204から無線ISO信号送受信部205を通して、無線同期チャンネル#`y`に送信する（ステップS517, S716）。

#### 【0105】

これを受信した無線ノード103は、キー`K`の値を使ってMPEG映像の値を復号化する（ステップS810）。復号化されたMPEGデータは、MPEGデコード部306にて復号化され、これをディスプレイ部307にて再生表示する。

#### 【0106】

このように、1394バスと無線網との間に代理ノードが存在するような相互接続の環境においても、エンドーエンドのノード同士（本実施形態では送信ノード101と無線ノード103）が認証手続きや鍵交換手続きを行うことができ、さらにその内容の中継ノード102を含め、その他のノードが知ることはできない仕組みとなっている。また、実際のMPEG映像等のコンテンツ保護の必要なデータの転送も、コピーが不可能なように経路の全てで暗号化されており、安全なデータ転送が可能になっている。これによって、このような相互接続の環境に

においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0107】

なお、以上の実施形態は、認証手続きや、暗号鍵の交換手続き等を、ノードのサブユニット単位で行ってきたが、無線ノード単位でこれを行うことも可能である。なお、ノード単位で行う例については、次の第2の実施形態で説明するので、例えばこれを適用すればよい。

【0108】

また、以上の実施形態では、認証および鍵交換のための手続きを暗号化データの受信後に行ってきたが、該手続きは、暗号化データ受信に先だって行ってももちろん構わない。例えば、装置や該当アプリケーションの立ち上げ時に該手続きを行ってもよい。

【0109】

(第2の実施形態)

次に、第2の実施形態について説明する。

【0110】

第1の実施形態では、送信ノードと無線ノードとが、直接、互いに認証手続きや鍵交換手続きを行ってきた。すなわち、送信ノード（の映像サブユニット）と無線ノード（のMPEGデコード/ディスプレイ機能）とが、直接、互いを認証し、暗号鍵の交換手続きを行って、暗号化データのやり取りを行ってきた。この際、中継ノードは、送信ノードに対しては無線ノードのMPEGデコード/ディスプレイ機能の代理機能を果たし、無線ノードに対しては送信ノードの映像送信サブユニットの代理機能を果たしてきたが、上記の認証手続きおよび暗号化データのやり取りの部分については、これらのデータの単なるフォワードを、代理していたサブユニットなり機能なりに行う形であった。

【0111】

これに対し、第2の実施形態では、中継ノードにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する場合の例を示す。すなわち、送信ノードと中継ノードとの間、および中継ノードと無線ノ

ードとの間で、各々のコピープロテクション手続きは閉じている。つまり、この実施形態においても、中継ノードは、送信ノードあるいは無線ノードに対して代理サービスは提供するものの、コピープロテクションについては、中継ノード自身が認証フォーマットを持ち、中継ノード自身が、1394バス区間のMPEGデータの暗号化転送についての責任を終端するとともに、無線区間のMPEGデータの暗号化転送についての責任を終端する場合の例である。

## 【0112】

図20に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第1の実施形態と同様である。

## 【0113】

図21に、送信ノード2101の内部構造の一例を示す。これも第1の実施形態と基本的には同様である。

## 【0114】

次に、図22に、中継ノード2102の内部構造の一例を示す。

## 【0115】

中継ノード2102は、第1の実施形態と同様に、IEEE1394バス側のノードに対して無線ノードの代理サーバとなり、無線ノードの機能を代理で提供する機能、および無線区間側のノードに対してIEEE1394バス側のノード（本実施形態では送信ノード2101）の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能を持つ。

## 【0116】

また、IEEE1394バス側から受信したデータ（MPEG映像データ）を無線区間側にフォワードする機能を持つが、第1の実施形態と相違する点は、認証データや暗号化等、コピープロテクションに関する手続きがIEEE1394バス区間と無線区間との両方について、この中継ノード2102において終端されており、IEEE1394バス側については認証フォーマットBcertをIEEE1394コピープロテクション処理部2208に、無線区間側については認証フォーマットCcertを無線区間コピープロテクション処理部2212にそれぞれ持ち、1394バスの同期チャネルから入力されてきた暗号化データに

については、ISO信号受信部2203にて受信→暗号復号化部2204にて暗号復号化→復号化されたMP EG映像を、暗号化部2205にて再暗号化→無線ISO信号送受信部2206にて、無線同期信号上に送信、というプロセスを踏む点である。

【0117】

ここで、AcertとBcertは、同じ認証機関（例えばIEEE1394のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述する無線区間の認証フォーマット（後述するCcertとDcert）については、同じくこの認証機関が発行したものであってもよいし、無線区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

【0118】

次に、図23に、無線ノード2103の内部構造の一例を示す。コピープロテクション処理部2303が、無線区間向けの認証フォーマットDcertを持っていること以外は、基本的には第1の実施形態の無線ノードと同様である。

【0119】

次に、実際のコピープロテクションを施した上でのMP EG映像全体のシーケンスについて、図24／図25（全体のシーケンス例）、図26／図27（送信ノード2101のフローチャート例）、図28／図29／図30（中継ノード2102のフローチャート例）、図31／図32（無線ノード2103のフローチャート例）を参照しながら説明する。

【0120】

まず、無線ノード2103は、自分の構成情報を中継ノード2102に通知する（ステップS2501）。構成情報とは、自分（無線ノード）がMP EGデコード／ディスプレイ機能を持つことといったことや、認証のための認証フォーマットを持っていることなどである（図14参照）。ここで、認証のための認証フォーマットが、無線区間用の認証フォーマットである旨を通知してもよい（ステップS2801）。

【0121】

これを受信した中継ノード 2102 は、無線ノード 2101 が認証フォーマットを持つことや、MPEG デコード／ディスプレイ機能を持っていることを確認する（ステップ S2701）。中継ノード 2102 は、第 1 の実施形態と同様に、この MPEG デコード／ディスプレイ機能を、IEEE 1212 レジスタや AV/C プロトコル等を使って、中継ノード 2102 自身のサブユニットとして IEEE 1394 バス側に広告する（ステップ S2502）。

【0122】

そのために、中継ノード 2102 は、代理サブユニット構成部 2210 内に代理テーブル 2214 を持つ。この代理テーブル 2214 は、基本的には第 1 の実施形態と同様であり、図 33／図 34 のように、中継ノード 2102 が代理で広告している形と、その実体との対応付けが記されているテーブルである。

【0123】

ここでは、図 33 のように、無線ノード 2103 の MPEG デコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップ S2702，S2703）。

【0124】

このため、送信ノード 2101 から見た中継ノード 2102 の構造は、図 35 のように見えることになる（ステップ S2702，S2703）。

【0125】

以上は、IEEE 1394 バス側についての説明であったが、第 1 の実施形態と同様に、これと同様の関係が無線区間にも成り立っている。すなわち、中継ノード 2102 は、IEEE 1394 バス側の機器やサービス、サブユニット構成等を調査し、これらの代理サービスを無線区間側に行っている。よって、図 34 のような設定がなされ、無線ノードから見た中継ノード 2102 の構造は図 36 のように見える。

【0126】

さて、中継ノード 2102 内に MPEG デコード／ディスプレイサブユニットがあると認識した送信ノード 2101 は、このサブユニットに対して、MPEG 映像を転送することを目的に、1394 バス上に同期チャンネル #x を確立し、

AV/Cプロトコルにて「この同期チャンネル# x（を受信するプラグ）と、MP EGデコード/ディスプレイサブユニットとを接続し、映像を表示せよ」との命令を出す（ステップS 2 5 0 3, S 2 6 0 2）。送信ノード2 1 0 1は、このサブユニットが中継ノード2 1 0 2にあるものと解釈しているため、命令の送信先は中継ノード2 1 0 2である。

## 【0 1 2 7】

これを受信（ステップS 2 7 0 4）した中継ノード2 1 0 2は、受信した命令パケットを解釈し、その命令が自らが代理サービスを行っているMP EGデコード/ディスプレイサブユニットに対する命令であることを認識し、代理テーブル2 2 1 0を参照して、この命令先の実体は無線ノード2 1 0 3にあることを認識する（ステップS 2 7 0 5）。

## 【0 1 2 8】

よって、I E E E 1 3 9 4バスの同期チャンネル# xを通して受信したデータを、無線ノード側にフォワードすべく、無線区間の同期チャンネル（# y）の確保を行い（ステップS 2 7 0 6）、さらにI S O信号送受信部2 2 0 3（同期チャンネル# xを受信）と無線I S O信号送受信部2 2 0 6（同期チャンネル# yを送信）を図2 2の点線のように接続し、1 3 9 4インタフェース2 2 0 1から入力された入力データを無線区間にそのままフォワードできるようにする（ステップS 2 5 0 4, S 2 7 0 7）。

## 【0 1 2 9】

さらに、無線ノード2 1 0 3に対して、「無線同期チャンネル# yを通してデータを送信するので、これを受信し、その結果をディスプレイに表示せよ」との命令を、無線ノード制御パケットの形（図1 9参照）で送信する（ステップS 2 5 0 5, S 2 7 0 8）。パケットの送信元は中継ノード2 1 0 2である。

## 【0 1 3 0】

これを受信した無線ノード2 1 0 3は、同期チャンネル# yを通してデータが送られてくることを認識する（ステップS 2 8 0 2）。

## 【0 1 3 1】

この後、送信ノード2 1 0 1は、同期チャンネル# xを通して、暗号化されたM

P E G映像を転送する（ステップ S 2 5 0 6）。これを受信した中継ノード 2 1 0 2 は、先に設定したようにこれをそのまま無線区間にフォワードする（ステップ S 2 7 0 9, S 2 5 0 7, S 2 5 0 8）。

#### 【0132】

このようにして、暗号化された M P E G映像が無線ノード 2 1 0 3 に到達する（ステップ S 2 8 0 3）が、この時点で無線ノード 2 1 0 3 はこの暗号を解くための鍵を有していないため、ここから暗号を解いて、M P E G映像を取り出すことはできない。ここで、無線ノード 2 1 0 3 は認証手続きが送信元との間で必要であることを認識する。

#### 【0133】

ここで、第 2 の実施形態の無線区間の暗号化の方式（プロトコル）は、I E E E 1 3 9 4 区間を含めて、第 1 の実施形態の暗号化方式と同様のメカニズムを持っているものとして、本実施形態の説明を行っていく。もちろん、認証方式のメカニズムは、本実施形態で示している方式に限定されるものではなく、他の種々の認証方式や暗号化方式にも適用が可能である。

#### 【0134】

さて、ここで、無線ノード 2 1 0 3（のコピープロテクション処理部 2 3 0 3）は、認証要求を暗号化データの送信元に対して送信する。先に述べたように、無線ノード 2 1 0 3 には、上記暗号化データの送信元は中継ノード 2 1 0 2（内の映像送信サブユニット）であるように認識されているので、認証要求の宛先も、中継ノード 2 1 0 2（内の映像送信サブユニット）である。ここで、認証手続きは、無線区間向けにあらかじめ定められたものであってもよい。その際、認証要求には、無線ノード 2 1 0 3 の認証フォーマット D c e r t を付与する（ステップ S 2 8 0 4, S 2 5 0 9）。

#### 【0135】

これを受信（ステップ S 2 7 1 0）した中継ノード 2 1 0 2 は、以下の 3 点を認識する。

#### 【0136】

1 点目は、先に無線同期チャネル # y を通して転送していたデータが暗号化さ

れており、IEEE 1394 バス区間と無線区間との両方において認証手続きと暗号鍵の取得が必要である点、2点目は、自分自身（中継ノード 2102）が、無線ノード 2103 との認証手続きを行うべきである、という点であり、3点目は、IEEE 1394 バス区間（中継ノード 2102 と送信ノード 2101）においても認証手続きを行うべきである、という点である。

【0137】

まず、中継ノード 2102 は、これを無線ノード 2103 から送られてきた認証要求であると解釈し、無線ノードとの認証手続きの手順を行う（ステップ S2509～S2512）。中継ノード 2102 は、同様の認証要求を、認証要求の送信元である無線ノード 2103 に対して行おうとする。この認証要求には、中継ノードの認証フォーマット `Ccert` が含まれる（ステップ S2711, S2510）。

【0138】

これを受け取った無線ノード 2103 は、これを中継ノード 2102 から送られてきた認証要求であると解釈する（ステップ S2805）。その後、この認証鍵の交換に必要な残りの手続きとして、無線ノード 2103 は、認証要求の中継ノード 2102 に対して認証手続きパケットを送信する（ステップ S2511）。この認証手続きパケットには、鍵交換初期値、署名等が含まれている（ステップ S2806）。

【0139】

これと同様の手続きが中継ノード 2101→無線ノード 2103 の方向に対しても行われる（ステップ S2512, S2713, S2807）。

【0140】

この認証手続きパケットを受信した中継ノード 2102 および無線ノード 2103 は、それぞれ、受信したパケットが改ざんされていないかどうかのタンパの確認、相手から送られてきた認証フォーマット型が正しいものであるかどうかの確認等を行い、与えられた値を使って共通の認証鍵 `Kauth2` を導き出す。この共通の認証鍵 `Kauth2` は、中継ノード 102 と無線ノード 103 との間で共通に持つ鍵で、この鍵 `Kauth2` を、この両者以外の他人に知られることな

く共有することがこの時点でできるようになる（ステップS2714，S2715，S2808）。

【0141】

以上は、無線区間における認証手続きである。同様の認証手続きが、IEEE1394バス区間においても行われる。具体的には、中継ノード2102のIEEE1394コピープロテクション処理部2208（認証フォーマットBcertを持っている）と、送信ノード2101のコピープロテクション処理部2403（認証フォーマットAcertを持っている）との間で行われる。手順としては、無線区間で行われた認証手続きと同様の手続きである（ステップS2513～S2516，S2604～S2609，S2717～S2721）。このようにして、送信ノード2101と中継ノード2102との間で共通の認証鍵kauth1を共有することになる。

【0142】

このように、無線区間、IEEE1394区間のそれぞれにおいて認証手続きが行われる。おのおのが終了すると、第1の実施形態と同様に、送信ノード2101と中継ノード2102との間でコンテンツキーK1が、中継ノード2102と無線ノード2103との間でコンテンツキーK2がそれぞれ共有されることになる。ここで、これ以外のノードには、これらのコンテンツキーの値は明らかになっていない。

【0143】

ここで、送信ノード101が、送信するMPEG映像を、コンテンツキーK1を使って、暗号化部2405にて暗号化し（ステップS2610）、これを1394バスの同期チャンネル#xを通して中継ノード102（のMPEGデコード／ディスプレイサブユニット）に対して送信する（ステップS2517，S2611）。

【0144】

中継ノード2102は、送信ノード2101から同期チャンネル#xを通して送られてくる、コンテンツキーK1で暗号化されたMPEG映像を、ISO信号送受信部2203にて受信すると、これを暗号復号化部2204に転送する（ステ

ップS2517, S2722)。この暗号復号化部2204では、先にIEEE1394区間でやり取りしたコンテンツキーK1の値をIEEE1394コピープロテクション処理部2208からもらい、暗号の復号化を行う（ステップS2518, S2723）。こうして取り出したMPEG映像を、今度は暗号化部2205に転送し、これも先に無線区間でやり直したコンテンツキーK2の値を使って暗号化し（ステップS2519, S2724）、無線ISO信号送受信部2206を通して、無線同期チャンネル#yに送信する（ステップS2520, S2725）。

【0145】

これを受信（ステップS2810）した無線ノード2103は、これを先に送られてきたKauth2を使ってコンテンツキーK2の値を導き出し、このキーK2の値を使ってMPEG映像の値を復号化する（ステップS2811）。復号化されたMPEGデータは、MPEGデコード部2306にて復号化され（ステップS2812）、これをディスプレイ部2307にて再生する（ステップS2813）。

【0146】

このように、IEEE1394バスと無線網の間に代理ノードが存在するような相互接続の環境においても、代理機能を提供する中継ノードと送信ノード、および中継ノードと受信ノードが、それぞれの区間で、認証手続きや鍵交換手続きを行うことで、実際のMPEG映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。これによって、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送が可能になる。

【0147】

もちろん、中継ノード2102の「生のMPEGデータ」が流れる部分、具体的には暗号復号化部2204と暗号化部2205との間には、データをコピーされる危険が考えられるため、この部分でデータコピーがなされないようにするための工夫（例えば、暗号復号化部と暗号化部を一体のLSIにするなど）がなされていると、この間でプローブをあてるなどしてデータを盗聴（不正コピー）す

ることが実質的に不可能になるため、このような対策を行っておくことが有益である。

【0148】

(第3の実施形態)

次に、第3の実施形態について説明する。

【0149】

第3の実施形態では、IEEE1394上において、HAVi規格 (Specification of the Home Audio/Vidio Interoperability (HAVi) Architecture) 等に代表される、AV/Cの上位レイヤに相当するAV機器制御ソフトウェアが稼働している場合における実施形態である。

【0150】

図37に、ある家庭のホームネットワークの全体構成の一例を示す。この全体構成は基本的には第1の実施形態と同様である。

【0151】

図38に、送信ノード4101の内部構造の一例を示す。これも第1の実施形態の場合とほぼ同様であるが、IEEE1212レジスタ4407を強調のため、追加記述している。IEEE1212レジスタ4407には、送信ノード4101の属性、例えば「どのベンダの製品かを示す情報、例えばVTRやチューナ等といったどのようなジャンルの製品かを示す情報、製造番号、制御ソフトウェアの配置URL、制御アイコン、コマンド一覧」等の情報が含まれる。

【0152】

次に、図39に、中継ノード4102の内部構造の一例を示す。中継ノード4102も、第1の実施形態とほぼ同様の構成であるが、本実施形態のシーケンスを説明する際に必要なIEEE1212レジスタ4213を1394バス構成認識部4206内に特に記した点と、HAVi処理部4212を持つ点が第1の実施形態と異なる。HAVi処理部4212には、いわゆるHAViバイトコードの処理を行う仮想マシン (VM) が存在する。また、本実施形態においては、制御画面の記述を行う「パネルサブユニット」の代理機能を代理サブユニット構成

部 4207 が持つ。

【0153】

次に、図 40 に、無線ノード 4103 の内部構造の一例を示す。これについても、第 1 の実施形態の場合と基本的には同様である。

【0154】

次に、H A V i 環境における、実際のコピープロテクションを施した上での M P E G 映像全体のシーケンスについて、図 41 / 図 42 (全体のシーケンス例)、図 43 / 図 44 (送信ノード 4101 のフローチャート例)、図 45 / 図 46 / 図 47 (中継ノード 4102 のフローチャート例)、図 48 / 図 49 (無線ノード 4103 のフローチャート例) を参照しながら説明する。

【0155】

まず、無線ノード 4103 は、自分の構成情報を中継ノード 4102 に通知する (ステップ S4501)。このとき、これらの構成情報は、I E E E 1212 レジスタ形式の情報として中継ノード 4101 に送付するものとする。すなわち、中継ノード 4102 が、無線ノード 4103 に対して「I E E E 1212 で規定される C S R (コマンド・ステータスレジスタ) 空間の、このアドレスに相当する部分についての情報」を要求し、これに無線ノード 4103 が答える形でこのやり取りが行われてもよい。ここで、前述のように、この構成情報には、自分 (無線ノード) が M P E G デコード / ディスプレイ機能を持つといったことや、認証のための認証フォーマットを持っていること、等が含まれる。ここで、無線ノード 4103 が持っている認証フォーマットを B c e r t とする。

【0156】

これを受信した中継ノード 4102 は、無線ノード 4101 が認証フォーマットを持つことや、M P E G デコード / ディスプレイ機能を持っていることを確認する (ステップ S4701)。中継ノード 4102 は、無線ノード 4101 が M P E G デコード / ディスプレイ機能を持っていることを I E E E 1394 バス側のノードに対して知らせるため、この M P E G デコード / ディスプレイ機能を、中継ノード 4102 自身のサブユニットとして I E E E 1394 バス側に広告する (ステップ S4502)。具体的には、自身の I E E E 1212 レジスタに「

自分はMPEGデコード／ディスプレイ機能を持っている」旨を記載したり、AV／Cプロトコルでサブユニット機能の問い合わせを受けた場合に、自分がMPEGデコード／ディスプレイサブユニットを持っているという形で応答を返したりする（これにより、送信ノード4101等のIEEE1394に接続されたノードは、中継ノードにこの機能が存在すると認識することになる）。

## 【0157】

そのために、中継ノード4102は、代理テーブル4208を持つ。代理テーブル4208は、図50／図51のように、中継ノード4102が代理で広告している形と、その実体との対応付けが記されているテーブルである。

## 【0158】

ここでは、図50のように、無線ノード4103のMPEGデコード／ディスプレイ機能が、中継ノード自身のサブユニットとして代理広告される（ステップS4702，S4703）。

## 【0159】

以上と逆の手続きがIEEE1394バス4104上の送信ノード4101の代理登録を無線区間側に対してみせる形で行われる（ステップS4503，S4504）。すなわち、送信ノード4101のIEEE1212レジスタ4407に、自分が映像送信機能を持つこと、およびパネル機能（制御画面機能）を持つことを記述しておき、これを中継ノード4102が読み込む（ステップS4601，S4704）。この送信ノード4101の機能を、中継ノード4102の機能として、代理して無線区間側のIEEE1212相当機能（無線区間側のCSR空間）に反映し、無線ノード4103側には、上記映像送信機能、およびパネル機能が中継ノード4102の機能であるものとして認識してもらう。この対応関係を、代理テーブル4208に図51のように反映する（ステップS4705）。

## 【0160】

このようにして代理テーブル4208は、図50／図51のように構成される。また、送信ノード4101から見た中継ノード4102の内部構造を図52に、無線ノード4103から見た中継ノード4102の内部構造を図53に、それ

ぞれ示す。

【0161】

なお、この時点で、ステップS4503の送信ノード構成情報の中に、送信ノード4101を制御するためのHAViのバイトコードが含まれており、中継ノード4102は送信ノード4101の代理サーバ、すなわちDCM（デバイスコントロールモジュール）の機能を有していてもよい。この場合、このバイトコードは、中継ノード4102のHAVi処理部4212内の仮想マシン上で稼働することになる。

【0162】

さて、中継ノード4102にパネル機能があるものと認識した無線ノード4103は、中継ノード4102の（パネルサブユニット）に対して、パネルの表示要求のコマンドを送出する（ステップS4505，S4802）。これを受信（ステップS4706）した中継ノード4102は、代理テーブル4208を参照し、このパネル機能の実体が送信ノード4101に存在していることを認識し、前記パネル表示要求コマンドを送信ノード4101に対してフォワードする（ステップS4506，S4707）。

【0163】

これを受信（ステップS4601）した送信ノード4101は、AV/Cプロトコルにてパネル応答（つまり、制御画面の送信）を行う。送信先は、中継ノード4102である（ステップS4603，S4507）。これを受信（ステップS4708）した中継ノード4102は、代理テーブル4208を参照して、これを無線ノード4103にフォワードする（ステップS4709，S4508，S4803）。

【0164】

ここで、図54に、無線ノード4103に送られてきた制御画面の一例を示す。この制御画面（パネル）では、6つの映画のタイトルを表示したボタンが提供される。これらのボタンは、例えば「ボタン1」、「ボタン2」、…等の名前が付けられており、ユーザがあるボタンを押すと、例えば「ボタン1が押されました」というコマンドの形で、パネルの送信元に送られる仕組みとなっているもの

とする。

#### 【0165】

さて、無線ノード4103は、中継ノード4102が提供していると認識している映像送信サービスを受けようと考え（実際に提供しているのは送信ノード4101）、無線ノード制御パケットを使って（ステップS4509）、映像を流すための無線同期チャンネル#yを確保し、このチャンネルを中継ノード4102の映像送信サブユニットに接続するためのコマンドを中継ノード4102に対して発行する（ステップS4804）。これを受信した中継ノード4102は、代理テーブル4208を参照して、実際にこのAV/Cコマンドが発行されるべきノード（送信ノード4191）を確認し、IEEE1394バス上に必要な帯域を確保するとともに（同期チャンネル#x）、内部のISO信号送受信部4204を設定して、IEEE1394バスの同期チャンネル#xと無線同期チャンネル#yとを相互に接続する（ステップS4710, S4711, S4712, S4510）。また、中継ノード4102は、送信ノード4101に対し、同期チャンネル#xを映像送信サブユニットに接続するコマンドを発行する（ステップS4511, S4713）。これを受信（ステップS4604）した送信ノード4101は、映像送信サブユニットの実体である内部の映像ストリームの流れるパス（図38で2重矢印になっている部分）をIEEE1394バスの同期チャンネル#xに接続する。

#### 【0166】

これと前後して、無線ノード4103のユーザは、見たい映像を選択するために図54のパネルの中から適当な番組を選択すべく、制御画面のボタンを押す（例えば、マウスを使ってクリックする、ペン入力する、タッチする、など）。この操作は、中継ノード4102に伝達され、これは代理テーブル4208の参照を経て送信ノード4101へのコマンドに変換される（ステップS4805, S4714, S4715, S4605, S4512, S4513）。

#### 【0167】

この後、送信ノード4101は、同期チャンネル#xを通して、暗号化されたMPEG映像を転送する（ステップS4514, S4606）。これは、中継ノード

ド 4 1 0 2 にて中継され、無線ノード 4 1 0 3 に到達する（ステップ S 4 7 1 6）。

【0168】

後の手続きは、第 1 の実施形態の場合と同様であり、暗号化された M P E G 映像が無線ノード 4 1 0 3 に到達する（ステップ S 4 8 0 6）が、この時点で無線ノード 4 1 0 3 はこの暗号を解くための鍵を有していないため、M P E G 映像の送信元と認証手続きを開始する。認証手続き以降の手続きについては第 1 の実施形態と同様であるので、ここでの詳細な説明は省略する。

【0169】

なお、第 1 の実施形態に従えば、認証は送信ノード 4 1 0 1 の映像送信サブユニットに相当する機能と、無線ノードの映像受信サブユニットに相当する機能ととの間で行われると考えられるが、第 3 の実施形態の場合には、このような認証方式の他に、送信ノード 4 1 0 1 のパネルサブユニットが認証の対象となるような方式も考えられる。この場合は、送信ノード 4 1 0 1 のパネルにデバイス ID が割り当てられることになる。

【0170】

なお、H A V i においては、送信ノード 4 1 0 1 から送られてくるバイトコードである D C M 等の中に、送信ノード 4 1 0 1 を制御するための制御画面情報が含まれる場合がある。このようなモジュールを D D I（データドリブンインタラクション）と呼ぶ。このようなモジュールは、例えば中継ノード 4 1 0 2 内の H A V i 処理部 4 2 1 2 にて展開され、制御画面が生成される。本実施形態では、この制御画面（あるいは、それと同等の機能を持つ制御画面）を無線ノード側に見せることを考える必要があるが、この場合は、代理サブユニット構成部 4 2 0 7 が、この D D I に含まれる画面構成情報を認識して（例えば、画面構成のためのシステムコールをイベントして認知して、生成される最終画面の概要を推察する方法や、完成した制御画面をもとにする方法等が考えられる）、パネルとしてこの制御画面を再構成し、無線区間に「パネルサブユニット」としてこれを公開する方法が考えられる。この場合には、代理テーブル 4 2 0 8 には、このパネルと、D D I で生成されるべき H A V i や A V / C のコマンド（中継ノード 4 1 0

2から送信ノード4101に対して発行される)の対応テーブルが用意されることになる。この方法は、無線ノード4103内にHAViバイトコードの仮想マシンが存在しなくても有効であるため、HAVi仮想マシンを持たない無線ノード4103から、HAVi機器の制御を可能とする方法である。

#### 【0171】

(第4の実施形態)

次に、第4の実施形態について説明する。

#### 【0172】

図55に、本実施形態の全体構成の一例を示す。

#### 【0173】

図55に示されるように、第4の実施形態では、ある家庭のホームネットワークであるIEEE1394バス6104と、公衆網(ここでは、一例としてインターネットとするが、電話網等でもよい)6105とが、ホームゲートウェイ6102で接続され、送信ノード6101と受信ノード6103との間で、認証手続き、暗号化の手続きを経た上で例えば映像データのやり取りを行う。ここで、インターネット6105(のアクセス網部分)は、IEEE1394バス6104と比べて通信帯域が非常に細く、IEEE1394バスでやり取りされる映像情報(一例としてMPEG2映像であるとする)は、帯域が足りずに通せないため、ホームゲートウェイ6102においてトランスコーディング、つまりMPEG2符号からMPEG4符号への符号変換を行った上で、伝送を行うことを考える。

#### 【0174】

第4の実施形態においても、第2の実施形態と同様に、ホームゲートウェイにて、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りを終端する。すなわち、送信ノードとホームゲートウェイ、ホームゲートウェイ受信ノードとで、おのおのコピープロテクション手続きは閉じている。この実施形態においても、ホームゲートウェイは、送信ノードや受信ノードに対して代理サービスを提供し、また、コピープロテクションについては、ホームゲートウェイ自身が認証フォーマットを持ち、ホームゲートウェイ自身が139

4 バス区間および無線区間のMPEGデータの暗号化転送についてのそれぞれの責任を終端する。

【0175】

次に、図56に、送信ノード6101の内部構造の一例を示す。これは基本的にはこれまでの実施形態と同様の構成である。

【0176】

次に、図57に、ホームゲートウェイ6102の内部構造の一例を示す。

【0177】

ホームゲートウェイ6102の基本的な構成は、無線インタフェースではなくインターネットインタフェース6202を有している点、代理サブユニット構成部ではなく代理ホームページ作成部6210を有している点、ホームページの作成・蓄積部6211を有している点、暗号復号化部6204と暗号化部6205との間にMPEG2/MPEG4変換部6214を有している点を除くと、第2の実施形態の中継ノードの構成とほぼ同様である。上記の相違点については順次説明していく。

【0178】

ホームゲートウェイ6102は、インターネット側のノードに対してIEEE1394バス側のノード（本実施形態では、送信ノード2101）の代理サーバとなり、IEEE1394バス側のノードの機能を代理で提供する機能を持つ。送信ノード6101が提供しているサービス（本実施形態の場合、映像送信サービス）には、ホームゲートウェイ6102が提供しているホームページを介してアクセスすることが可能である。ここで、受信ノード6103からは、送信ノード6101のサービスは、ホームゲートウェイ6102のホームページを介して見えるため、これをホームゲートウェイ6102が提供するIP（インターネット）上のサービスとして解釈されてもよい。

【0179】

また、ホームゲートウェイ6102は、第2の実施形態と同様に、IEEE1394バス側から受信したデータ（MPEG2映像データ）をインターネット側にフォワードする機能を持つが、認証やデータの暗号化等、コピープロテクショ

ンに関する手続きが I E E E 1 3 9 4 バス区間とインターネット区間との両方について、このホームゲートウェイにおいて終端されている。I E E E 1 3 9 4 バス側については、認証フォーマット B c e r t を I E E E 1 3 9 4 コピープロテクション処理部 6 2 0 8 に、インターネット区間側については、認証フォーマット C c e r t をインターネット側コピープロテクション処理部 6 2 1 2 にそれぞれ持ち、I E E E 1 3 9 4 バスの同期チャネルから入力されてきた暗号化データについては、I S O 信号送受信部 6 2 0 3 にて受信→暗号復号化部 2 2 0 4 にて暗号復号化→復号化された M P E G 2 映像を M P E G 2 / M P E G 4 変換部 6 2 1 4 にてトランスコード→M P E G 4 映像を暗号化部 6 2 0 5 にて再暗号化→A V 信号送受信部 6 2 0 6 にてインターネット側に送信、というプロセスを踏む。

ここで、A c e r t と B c e r t は、同じ認証機関（例えば I E E E 1 3 9 4 のコピープロテクションを担当する認証機関）が発行した認証フォーマットであると仮定するが、後述するインターネット区間の認証フォーマット（後述する C c e r t と D c e r t ）については、同じくこの認証機関が発行したものであってもよいし、インターネット区間を担当する別の認証機関が発行する認証フォーマットであってもよい。

#### 【0180】

次に、図 5 8 に、受信ノード 6 1 0 3 の内部構造の一例を示す。

#### 【0181】

コピープロテクション処理部 6 3 0 3 がインターネット向けの認証フォーマット D c e r t を持っている。第 2 の実施形態との相違点は、インタフェース（インターネットインタフェース 6 3 0 1、制御パケット送受信部 6 3 0 2、A V 信号送受信部 6 3 0 4）がインターネット対応となっている点である。ここで、制御パケット送受信部 6 3 0 2 は T C P、A V 信号送受信部 6 3 9 4 は U D P のトランスポートプロトコルを持つパケットの送受信モジュールであってもよい。

#### 【0182】

次に、実際のコピープロテクションを施した上での映像送信全体のシーケンスについて、図 5 9 / 図 6 0（全体のシーケンス例）、図 6 1（送信ノード 6 1 0 3 のフローチャート例）、図 6 2 / 図 6 3（ホームゲートウェイ 6 1 0 2 のフロ

ーチャート例)、図64(受信ノード6103のフローチャート例)を参照しながら説明する。

【0183】

まず、ホームゲートウェイ6102は、送信ノード6101のIEEE1212レジスタの読み込みなどを通して、送信ノードについての属性や構成情報を収集する(ステップS6501, S6601, S6701, S6502, S6602, S6702)。これを通して、ホームゲートウェイ6102は、送信ノード6101が映像送信機能を持つこと、パネル機能を持つこと、認証フォーマットを持っていること等を把握する。

【0184】

これを受けて、ホームゲートウェイ6102は、送信ノード6101を遠隔制御するためのホームページを作成する(ステップS6503)。基本的には、送信ノード6101が持つパネルと同様の画面を「送信ノード制御用ホームページ」として作成する。ホームページ上に配置された制御用のボタン等は、それぞれ送信ノード6101のパネルサブユニットのボタンに対応する等して、代理ホームページ作成部6210内の変換テーブルに対応の一覧が記述される。例えば、送信ノード6101のパネルサブユニットに「再生」とかかかれているボタンが存在する場合には、該ホームページにも「再生」とかかかれているボタンを用意して、この関係を前記変換テーブルに記述しておく。もし、このホームページのユーザがこのボタンを押した場合には、ホームゲートウェイ6102から送信ノード6101のパネルサブユニットの「再生」ボタンに対して「ボタンが押された」というインタラクションが返る形となる。図65(a)に送信ノード6101のパネルサブユニットの持つパネルの一例を、図65(b)にホームゲートウェイ6102の作成した送信ノード制御用ホームページの一例をそれぞれ示す。

【0185】

さて、インターネット上の受信ノード6103は、インターネットを介してこのホームゲートウェイ6201にアクセスし、送信ノード6101の制御画面を含むホームページを要求し、このホームページが送付される(ステップS6504, S6801, S6703)。これを見て、受信ノード6103のユーザは、

画面上の映像送信を要求するボタン（例えば、図65（b）の「再生」ボタン）を押したものとする。この結果、例えば「再生ボタンが押された」、というインタラクションが、インターネット経由でホームゲートウェイにHTTPを通じて通知される（ステップS6505, S6802, S6704）。

## 【0186】

これを受信したホームゲートウェイ6102は、受信した命令を解釈し、その命令が、自らがホームページを通じて代理サービスを行っている送信ノード6101の映像送信サブユニット、およびパネルサブユニットに対する命令であることを認識する。よって、IEEE1394上に映像送信のための同期チャンネル#xを確保し、この同期チャンネルを送信ノードの映像送信サブユニットと接続する手続きを行う。また、送信ノード6101のパネルサブユニットに対して、「再生」に該当するボタンを押すことを意味するコマンドを送信する（ステップS6506, S6705）。

## 【0187】

これを受信した送信ノード6101は、同期チャンネル#xを通して、暗号化されたMPEG2映像を送出する（ステップS6507）。第2の実施形態においては、中継ノードは送られてきたMPEG映像をそのまま無線ノードにフォワーディングしていたが、本第4の実施形態においては、内部でMPEG4からMPEG2にトランスコードしなくてはならないため、MPEG2映像はホームゲートウェイ6102内にて復号化される必要がある。ところが、この時点でホームゲートウェイ6102は、この暗号を解くための鍵を有していないため、ここから暗号を解いて、MPEG2映像を取り出すことはできない。ここで、ホームゲートウェイ6102は、認証手続きが送信元との間で必要であることを認識する（ステップS6508, S6706）。

## 【0188】

しかしながら、ホームゲートウェイ6102は、これから受信ノード6103に転送しようとしているデータが、認証手続きが必要なコンテンツであることを認識し、まず、受信ノード6103が信頼に足るノードであるのかをまず確かめるべく、ホームゲートウェイ6102と受信ノード6103との間で認証手続き

を行う（ステップS6707, S6509, S6510）。このようにすることにより、未然に悪意ユーザに対するコンテンツの送信を、いずれの符号化形式、あるいはいずれの接続ネットワークのいかんを問わず、行うことができる。

## 【0189】

この認証・鍵交換手続きは、第2の実施形態のIEEE1394上の認証・鍵交換手続きをインターネット上で行ってもよいし、ISPEC等のインターネット上で定められた認証・鍵交換手続きにてこれを行ってもよい。

## 【0190】

具体的には、ホームゲートウェイ6102は、受信ノード6103巻の認証手続きが終了すると、受信ノード6103が信頼に足るノードであることを確認し、映像を送信しても大丈夫であると判断し、次に自身と送信ノード6101との認証手続きにはいる。具体的には、ホームゲートウェイ6102は、送信ノード6101に対して、認証要求を送信する（ステップS6511, S6709, S6605）。これに引き続き、ホームゲートウェイ6102と送信ノード6101との間において、認証手続きが行われる（ステップS6512, S6710, S6606）。この認証手続きについても、これまでの実施形態で行われてきた認証手続きと同様の手続きが行われてもよい。

## 【0191】

以上のようにして、認証が終了したノード間において、コンテンツの暗号化を行う鍵についての情報が共有される。送信ノード2101とホームゲートウェイ6102との間でコンテンツキーK1が、ホームゲートウェイ6102と受信ノード6103との間でコンテンツキーK2がそれぞれ共有されることになる。

## 【0192】

ここで、送信ノード6101が、送信するMPEG2映像を、コンテンツキーK1を使って、暗号化部6405にて暗号化し（ステップS6607）、これを1394バスの同期チャンネル#xを通してホームゲートウェイ6102に対して送信する（ステップS6608, S6513）。

## 【0193】

ホームゲートウェイ6102は、送信ノード6101から同期チャンネル#xを

通して送られてくる、コンテンツキー K1 で暗号化された M P E G 2 映像を、I S O 信号送受信部 6 2 0 3 にて受信すると、これを暗号復号化部 6 2 0 4 に転送する（ステップ S 6 7 1 1）。この暗号復号化部 6 2 0 4 では、先に I E E E 1 3 9 4 区間でやり取りしたコンテンツキー K1 の値を I E E E 1 3 9 4 コピープロテクション処理部 6 2 0 8 からもらい、暗号の復号化を行う（ステップ S 6 5 1 4, S 6 7 1 2）。こうして取り出した M P E G 2 映像を、M P E G 2 / M P E G 4 変換部 6 2 1 4 にて符号変換を行い、インターネットでも送信しうる帯域に帯域圧縮を行う（ステップ S 6 5 1 5, S 6 7 1 3）。M P E G 4 符号化されたデータは、暗号化部 6 2 0 5 に転送され、これも先にインターネット区間でやり取りしたコンテンツキー K2 の値を使って暗号化し（ステップ S 6 5 1 6, S 6 7 1 4）、A V 信号送受信部 6 2 0 6 を通して、インターネット側に送信する（ステップ S 6 5 1 7, S 6 7 1 5）。

【0194】

ここで、ホームゲートウェイ 6 1 0 2 の暗号復号化部 6 2 0 4 から M P E G 2 / M P E G 4 変換部 6 2 1 4 を経由して、暗号化部 6 2 0 5 にかけては生の M P E G 2 または M P E G 4 データが流れることになるので、不正コピーがなされないように保護がなされている（例えば、暗号化復号化部と M P E G 2 / M P E G 4 変換部、暗号化部を一体の L S I にするなど）のが望ましい。

【0195】

さて、これを受信（ステップ S 6 8 0 5）した受信ノード 6 1 0 3 は、これを先に作成した鍵情報（K2）を使って M P E G 4 映像の値を復号化する（ステップ S 6 8 0 6）。復号化された M P E G 4 データは、M P E G デコード部 6 3 0 6 にて復号化され（ステップ S 6 8 0 7）、これをディスプレイ部 6 3 0 7 にて再生する（ステップ S 6 8 0 8）。

【0196】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイと送信ノード、およびホームゲートウェイと受信ノードが認証手続きや鍵交換手続きを行うことで、実際の M P E G 映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで

暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

【0197】

(第5の実施形態)

次に、第5の実施形態について説明する。

【0198】

第4の実施形態が、公衆網（インターネット）を介して家庭網にアクセスし、コピープロテクションを考慮した上で家庭網上の端末とインターネット上の端末間でコンテンツをやり取りする場合であったのに対し、第5の実施形態は、公衆網を介して家庭網間でコンテンツをやり取りする場合である。

【0199】

図66に、本実施形態の全体構成図を示す。

【0200】

図66に示されるように、第5の実施形態では、2つの家庭網8105、8107が公衆網（ここでは、一例としてインターネットとするが、B-ISDN等でもよい）8106にて接続されている。第1の家庭網8105上の送信ノード8101から、コピープロテクションを考慮した形で、AVコンテンツを第2の家庭網8107上の受信ノード8104に送信する。ここで、第4の実施形態では、公衆網部分の通信帯域が非常に細い場合の例を示したが、本実施形態では、公衆網の通信帯域は十分な容量を持つものとする。

【0201】

第5の実施形態においては、第1の実施形態の中継ノードと同様に、ホームゲートウェイ8102、8103にて、IEEE1394バス8105、8107上のサービスを公衆網側に代理サービスする。すなわち、インターネット上からは、インターネットのサービスとして、家庭網上の装置やサービス、コンテンツが見える。また、ホームゲートウェイ8102、8103は、一連のコピープロテクション手続き、すなわち認証手続きや暗号化データのやり取りについてはこれらをフォワードする。

【0202】

送信ノード8101や受信ノード8104は、基本的には第4の実施形態と同様の構成である。

【0203】

図67に、ホームゲートウェイ8102、8103の内部構造の一例を示す。

ホームゲートウェイ8102の基本的な構成は、コピープロテクションを終端しない点（これは、第1の実施形態の中継ノードと同様）、および暗号の符号化・復号化・符号変換を行わない点（これも、第1の実施形態の中継ノードと同様）を除き、第4の実施形態のホームゲートウェイの構成とほぼ同様である。

【0204】

図68に、全体のシーケンスの一例を示す。

【0205】

ここでは、第2の家庭網8107のユーザが、ホームゲートウェイ8103の制御画面を使って、送信ノード8101のコンテンツを、インターネット8106を介して受信ノード8104に配信させる場合を考える。

【0206】

まず、第4の実施形態と同様に、ステップS8301の構成認識と、ステップS8302の送信ノード制御用ホームページ作成が行われる。

【0207】

第2の家庭網8107のユーザは、ホームゲートウェイ8103を操作し、ホームゲートウェイ8102から送信ノード制御用のホームページ（制御画面）を持ってくる（ステップS8303）。また、例えば図69に例示するような受信ノード8104の制御画面も同時に開く。そこで、図69のように、送信ノード内のコンテンツ一覧から、適当なものを例えばドラッグアンドドロップするなどして、ホームゲートウェイ8103に映像配信を命令する（ステップS8304）。

【0208】

すると、第4の実施形態と同様に、映像送信要求がホームゲートウェイ8102に（インターネットコマンドとして）発行され（ステップS8305）、これ

がホームゲートウェイ8102にてAV/Cプロトコルコマンドに翻訳され、送信ノード8101から受信ノード8104間の通信パス（IEEE1394バス8105上の同期チャンネル#x、インターネット上のコネクション、IEEE1394バス上の同期チャンネル#y）が設定される（ステップS8306、S8307）。この上を、暗号鍵Kで暗号化されたMPEG2映像が配信される（ステップS8308～S8310）。

【0209】

第1の実施形態と同様に、これを受信した受信ノード8106は、送信元に認証要求を発行する（ステップS8311）。受信ノード8104は、この映像はホームゲートウェイ8103から配信されていると解釈しているため、この認証要求はホームゲートウェイ8103に対して行われる。

【0210】

ホームゲートウェイ8103は、第4の実施形態と同様に、内部の変換テーブル8211を参照して、これをホームゲートウェイ8102にフォワードする。これは、ホームゲートウェイ8103は、映像の配信元がホームゲートウェイ8102であると解釈しているからである。このフォワードは、認証要求8311の中身を変えない形で、インターネットパケットで行われる（ステップS8312）。同様に、ホームゲートウェイ8102は、これを受信ノード8101にフォワードする（ステップS8313）。送信ノード8101は、これをホームゲートウェイ8101から発行された認証要求であると解釈する。

【0211】

これと同様の手順を双方向に組み、送信ノード8101と受信ノード8104間で認証手続きが行われる（ステップS8314）。この間、ホームゲートウェイは、この手続きのパケットの中身を変更せずにフォワードする。認証と並行して、鍵情報のやり取りを行い、受信ノード8104は鍵の入手を行い、結局、暗号化されたMPEG2映像の復号化ができるようになる。

【0212】

しかして、送信ノード8101が送信するMPEG映像を、コンテンツキーKを使って暗号化し、これが1394バスの同期チャンネル#x、ホームゲートウェイ

イ 8102、公衆網、ホームゲートウェイ 8103、1394バスの同期チャンネル #y という経路を辿って、受信ノード 8103 に到達する（ステップ S8315～S8317）。そして、受信ノード 8103 では、暗号化された MPEG 映像は、暗号鍵 K を使って暗号復号化され、デコードされて、再生表示される。

#### 【0213】

このように、家庭網とインターネットが相互接続された環境においても、代理機能を提供するホームゲートウェイを介して、送信ノードと受信ノードが認証手続きや鍵交換手続きを行うことで、実際の MPEG 映像等のコンテンツ保護の必要なデータの転送を、コピーが不可能なように経路の全てで暗号化されて行うことができ、安全なデータ転送が可能になっている。このように、このような相互接続の環境においても、コピープロテクションを考慮したデータ転送を行うことが可能になる。

#### 【0214】

なお、第 5 の実施形態において、公衆網の通信帯域が十分に広くない場合には、両ホームゲートウェイにおいて第 4 の実施形態の符号化変換（例えば、ホームゲートウェイ 8102 では MPEG2/MPEG4 変換、ホームゲートウェイ 8103 では MPEG4/MPEG2 変換）を行うことによって、若干の圧縮損はあるものの、両家庭網間でコピープロテクションを考慮したデータ転送を行うことが可能になる。

#### 【0215】

なお、第 1～第 5 の実施形態において例示したデータ転送の方向とは逆の方向にデータ転送する場合（例えば、無線ノードから IEEE1394 上のノードへデータ転送する場合）にも、本発明は適用可能である。

#### 【0216】

また、第 1～第 5 の実施形態において、無線ノードや IEEE1394 上のノードについては、コンテンツについて送信機能または受信機能の一方に着目して説明したが、無線ノードや IEEE1394 上のノードは、コンテンツについて送信機能と受信機能の両方を備えることも可能である。

#### 【0217】

また、認証手続きや、鍵交換手続き（コンテンツ鍵共有手続き）は、これまでに例示したものに限定されず、他の種々の方法が用いられる場合にも本発明は適用可能である。

【0218】

また、以上では、家庭網ネットワークとして実施形態を説明したが、もちろん、本発明は家庭網以外のネットワークにも適用可能である。

【0219】

なお、以上の各機能は、ソフトウェアとしても実現可能である。

【0220】

また、本実施形態は、コンピュータに所定の手段を実行させるための（あるいはコンピュータを所定の手段として機能させるための、あるいはコンピュータに所定の機能を実現させるための）プログラムを記録したコンピュータ読取り可能な記録媒体としても実施することもできる。

【0221】

本発明は、上述した実施の形態に限定されるものではなく、その技術的範囲において種々変形して実施することができる。

【0222】

【発明の効果】

本発明によれば、同じネットワークでは接続されていない装置間で、保護すべきコンテンツの送受信のためのコンテンツ保護手続きを行うことが可能になる。

【図面の簡単な説明】

【図1】

本発明の第1の実施形態に係るネットワークの全体構成の一例を示す図

【図2】

送信ノードの内部構造の一例を示す図

【図3】

中継ノードの内部構造の一例を示す図

【図4】

無線ノードの内部構造の一例を示す図

【図 5】

全体のシーケンスの一例を示す図

【図 6】

全体のシーケンスの一例を示す図

【図 7】

送信ノードの動作手順の一例を示すフローチャート

【図 8】

送信ノードの動作手順の一例を示すフローチャート

【図 9】

中継ノードの動作手順の一例を示すフローチャート

【図 10】

中継ノードの動作手順の一例を示すフローチャート

【図 11】

中継ノードの動作手順の一例を示すフローチャート

【図 12】

無線ノードの動作手順の一例を示すフローチャート

【図 13】

無線ノードの動作手順の一例を示すフローチャート

【図 14】

無線ノード構成情報パケットの一例を示す図

【図 15】

代理テーブルの一例を示す図

【図 16】

代理テーブルの一例を示す図

【図 17】

送信ノードから見た中継ノードの内部構造を説明するための図

【図 18】

無線ノードから見た中継ノードの内部構造を説明するための図

【図 19】

無線ノード制御パケットの一例を示す図

【図 20】

本発明の第 2 の実施形態に係るネットワークの全体構成の一例を示す図

【図 21】

送信ノードの内部構造の一例を示す図

【図 22】

中継ノードの内部構造の一例を示す図

【図 23】

無線ノードの内部構造の一例を示す図

【図 24】

全体のシーケンスの一例を示す図

【図 25】

全体のシーケンスの一例を示す図

【図 26】

送信ノードの動作手順の一例を示すフローチャート

【図 27】

送信ノードの動作手順の一例を示すフローチャート

【図 28】

中継ノードの動作手順の一例を示すフローチャート

【図 29】

中継ノードの動作手順の一例を示すフローチャート

【図 30】

中継ノードの動作手順の一例を示すフローチャート

【図 31】

無線ノードの動作手順の一例を示すフローチャート

【図 32】

無線ノードの動作手順の一例を示すフローチャート

【図 33】

代理テーブルの一例を示す図

【図 34】

代理テーブルの一例を示す図

【図 35】

送信ノードから見た中継ノードの内部構造を説明するための図

【図 36】

無線ノードから見た中継ノードの内部構造を説明するための図

【図 37】

本発明の第3の実施形態に係るネットワークの全体構成の一例を示す図

【図 38】

送信ノードの内部構造の一例を示す図

【図 39】

中継ノードの内部構造の一例を示す図

【図 40】

無線ノードの内部構造の一例を示す図

【図 41】

全体のシーケンスの一例を示す図

【図 42】

全体のシーケンスの一例を示す図

【図 43】

送信ノードの動作手順の一例を示すフローチャート

【図 44】

送信ノードの動作手順の一例を示すフローチャート

【図 45】

中継ノードの動作手順の一例を示すフローチャート

【図 46】

中継ノードの動作手順の一例を示すフローチャート

【図 47】

中継ノードの動作手順の一例を示すフローチャート

【図 48】

無線ノードの動作手順の一例を示すフローチャート

【図 49】

無線ノードの動作手順の一例を示すフローチャート

【図 50】

代理テーブルの一例を示す図

【図 51】

代理テーブルの一例を示す図

【図 52】

送信ノードから見た中継ノードの内部構造を説明するための図

【図 53】

無線ノードから見た中継ノードの内部構造を説明するための図

【図 54】

無線ノードに送られてきた制御画面の一例を示す図

【図 55】

本発明の第4の実施形態に係るネットワークの全体構成の一例を示す図

【図 56】

送信ノードの内部構造の一例を示す図

【図 57】

ホームゲートウェイの内部構造の一例を示す図

【図 58】

受信ノードの内部構造の一例を示す図

【図 59】

全体のシーケンスの一例を示す図

【図 60】

全体のシーケンスの一例を示す図

【図 61】

送信ノードの動作手順の一例を示すフローチャート

【図 62】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図 63】

ホームゲートウェイの動作手順の一例を示すフローチャート

【図 64】

受信ノードの動作手順の一例を示すフローチャート

【図 65】

送信ノードのパネルとホームゲートウェイの送信ノード制御用ホームページの一例を示す図

【図 66】

本発明の第 5 の実施形態に係るネットワークの全体構成の一例を示す図

【図 67】

ホームゲートウェイの内部構造の一例を示す図

【図 68】

全体のシーケンスの一例を示す図

【図 69】

制御画面の一例を示す図

【符号の説明】

101, 2101, 4101, 6101, 8101…送信ノード

102, 2102, 4102…中継ノード

103, 2103, 4103, 6104…無線ノード

6102, 8102, 8103…ホームゲートウェイ

6103, 8104…受信ノード

104, 2104, 4104, 8105, 8107…IEEE1394バス

6105, 8106…公衆網

201, 2201, 4201, 6201, 8201…IEEE1394インタフェース

202, 2202, 4202…無線インタフェース

203, 2207, 4203, 6207, 8203…AV/Cプロトコル処理部

204, 2203, 4204, 6203, 8204…ISO信号送受信部

205, 2206, 4205…無線ISO信号送受信部  
 206, 2209, 4206, 6209…1394バス構成認識部  
 207, 2210, 4207, 8207…代理サブユニット構成部  
 208, 2214, 4208, 6215…代理テーブル  
 209, 2211, 4209…無線区間構成認識部  
 210, 4210, 8209…コピープロテクション制御/フォワード部  
 2208, 6208…IEEE1394コピープロテクション処理部  
 2212…無線区間コピープロテクション部  
 8211…変換テーブル  
 211, 2213, 4211…無線ノード制御パケット送受信部  
 2204, 6204…暗号復号化部  
 2205, 6205…暗号化部  
 4212…HAVi処理部  
 4213…IEEE1212レジスタ  
 6206, 8205…AV信号送受信部  
 6202, 8202…インターネットインタフェース  
 6210, 8208…代理ホームページ作成部  
 6211, 8210…ホームページ作成・蓄積部  
 6212…インターネット側プロテクション処理部  
 6213…制御パケット送受信部  
 6214…MPEG2/MPEG4変換部  
 6206…制御パケット処理部  
 301, 2301, 4301…無線インタフェース  
 302, 2302, 4302…無線ノード制御パケット送受信部  
 303, 2303, 4303, 6303…コピープロテクション処理部  
 304, 2304, 4304…無線ISO信号送受信部  
 305, 2305, 4305, 6305…暗号復号化部  
 306, 2306, 4306, 6306…MPEGデコード部  
 307, 2307, 4307, 6307…ディスプレイ部

6301…インターネットインタフェース

6302…制御パケット送受信部

6304…AV信号送受信部

401, 2401, 4401, 6401…IEEE1394インタフェース

402, 2402, 4402, 6402…AV/Cプロトコル処理部

403, 2403, 4403, 6403…コピープロテクション処理部

404, 2404, 4404, 6404…ISO信号送受信部

405, 2405, 4405, 6405…暗号化部

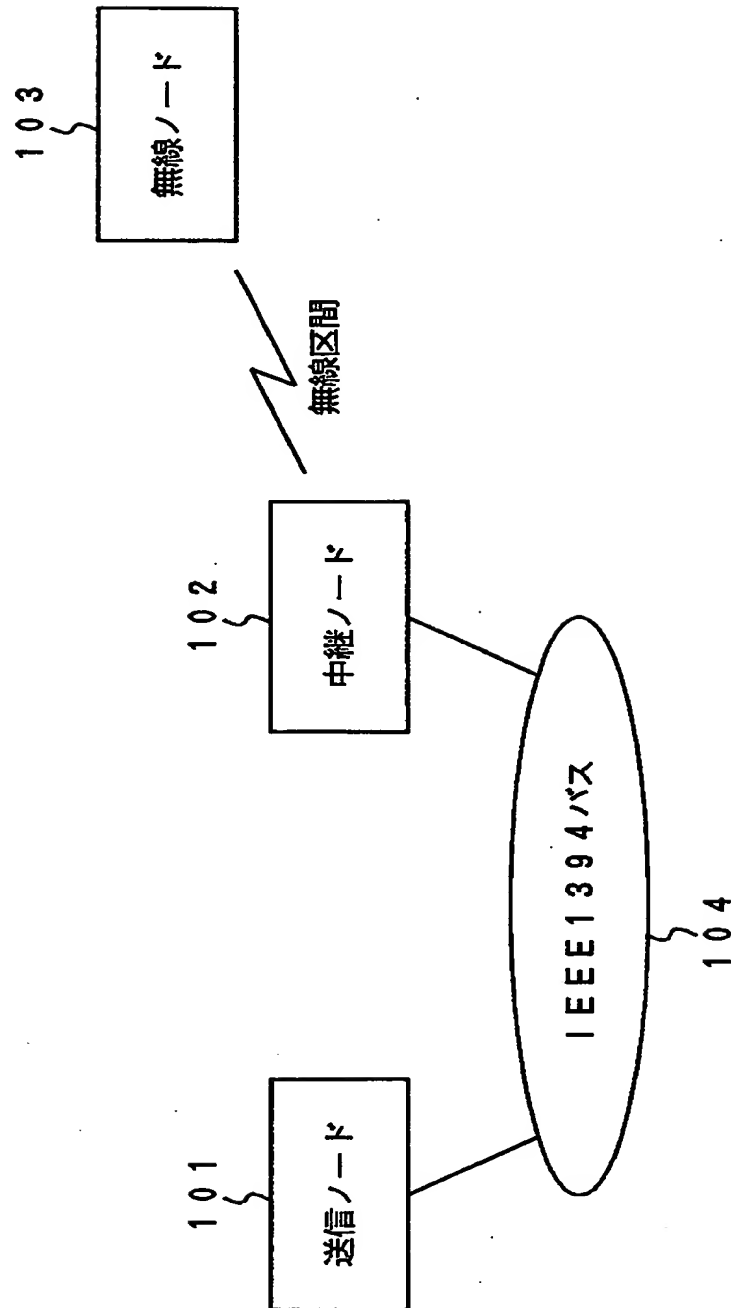
406, 2406, 4406, 6406…MPEGストレージ部

4407…IEEE1212レジスタ

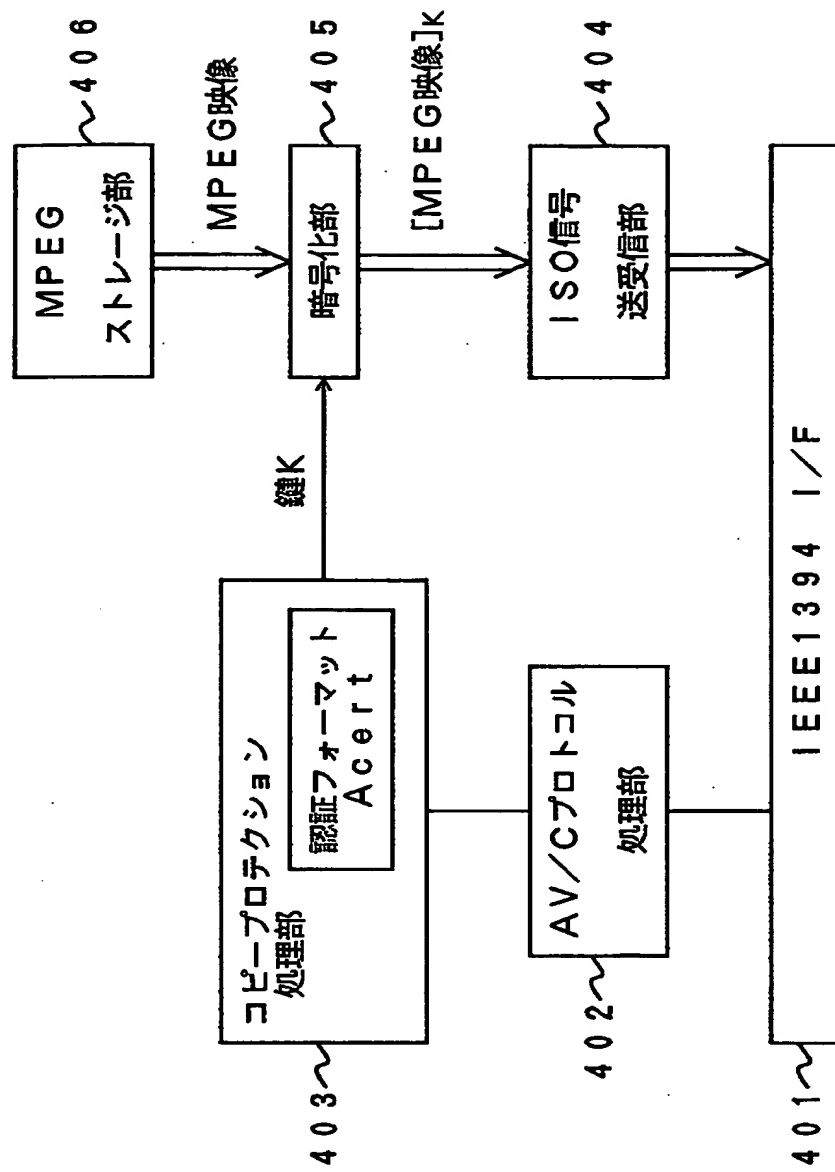
【書類名】

図面

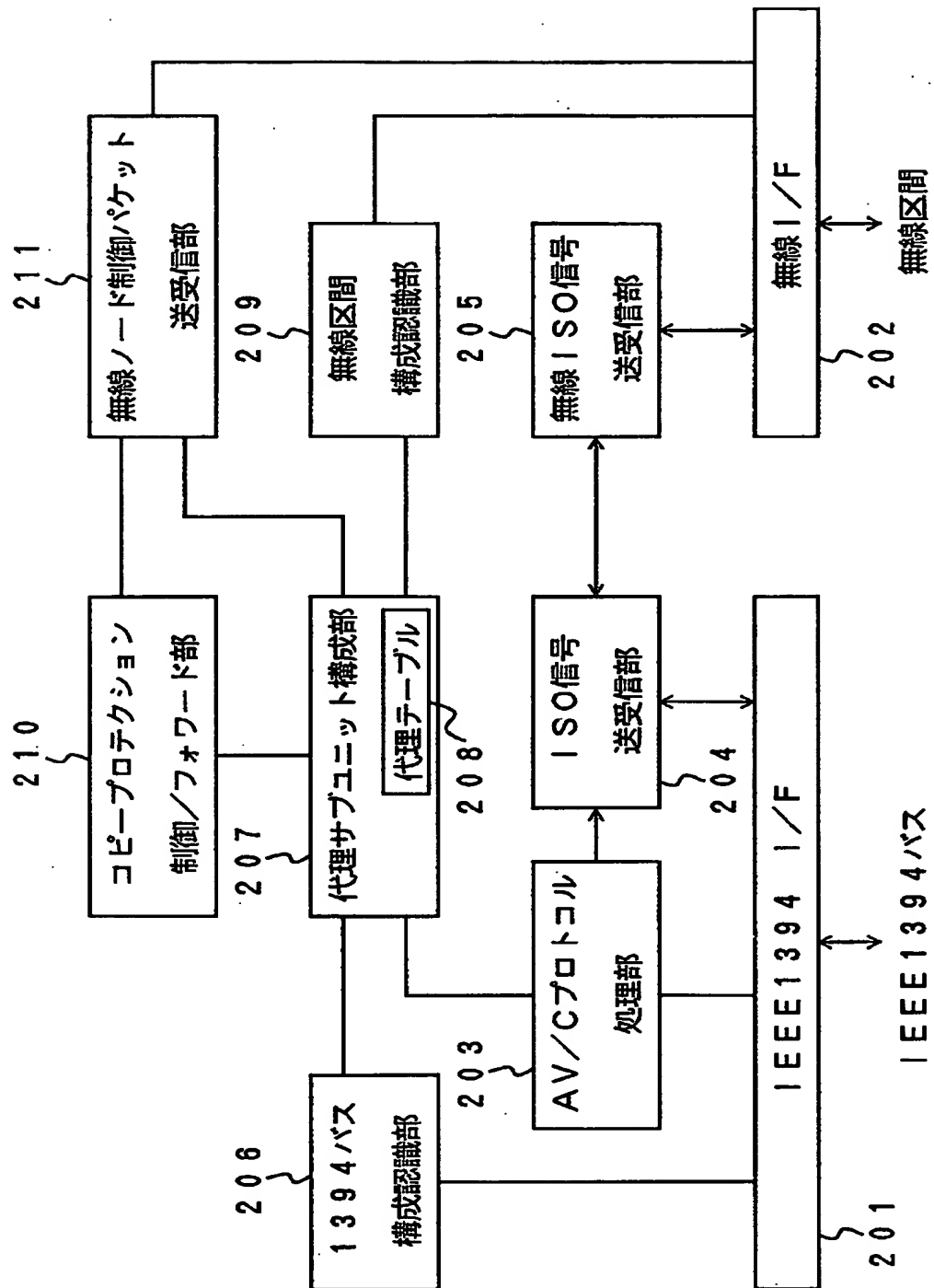
【図 1】



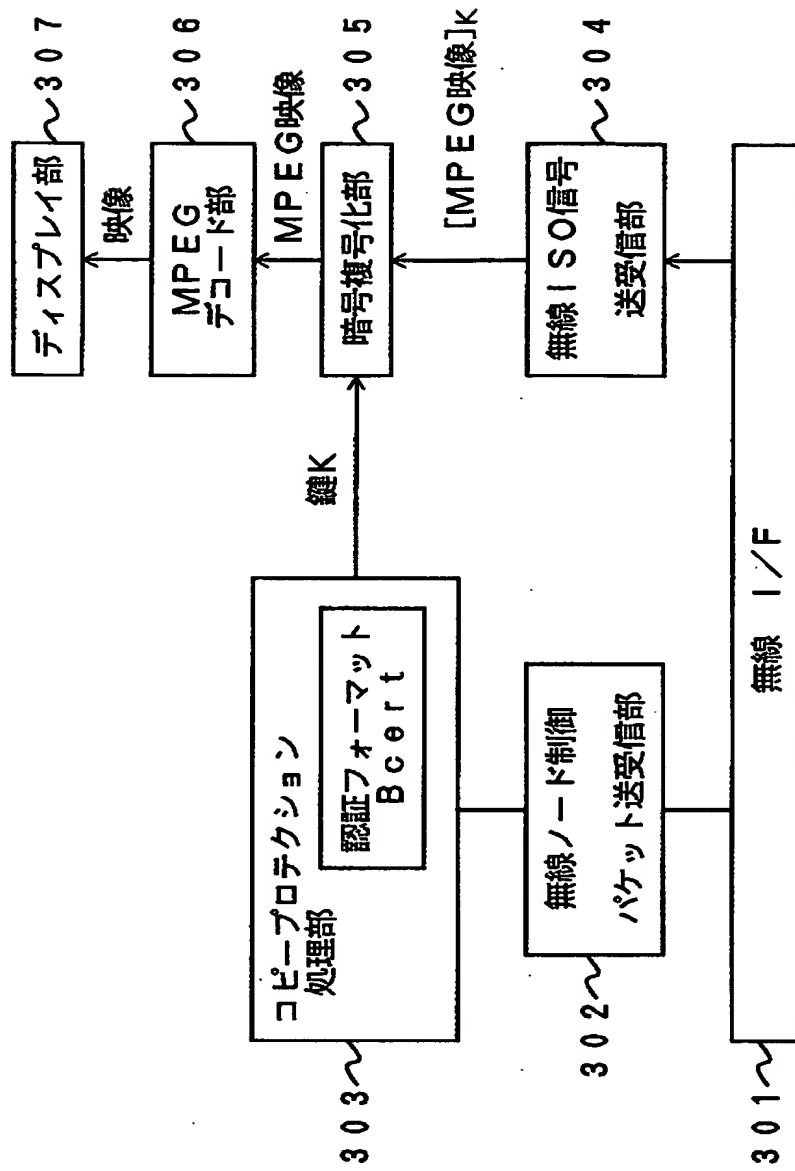
【図 2】



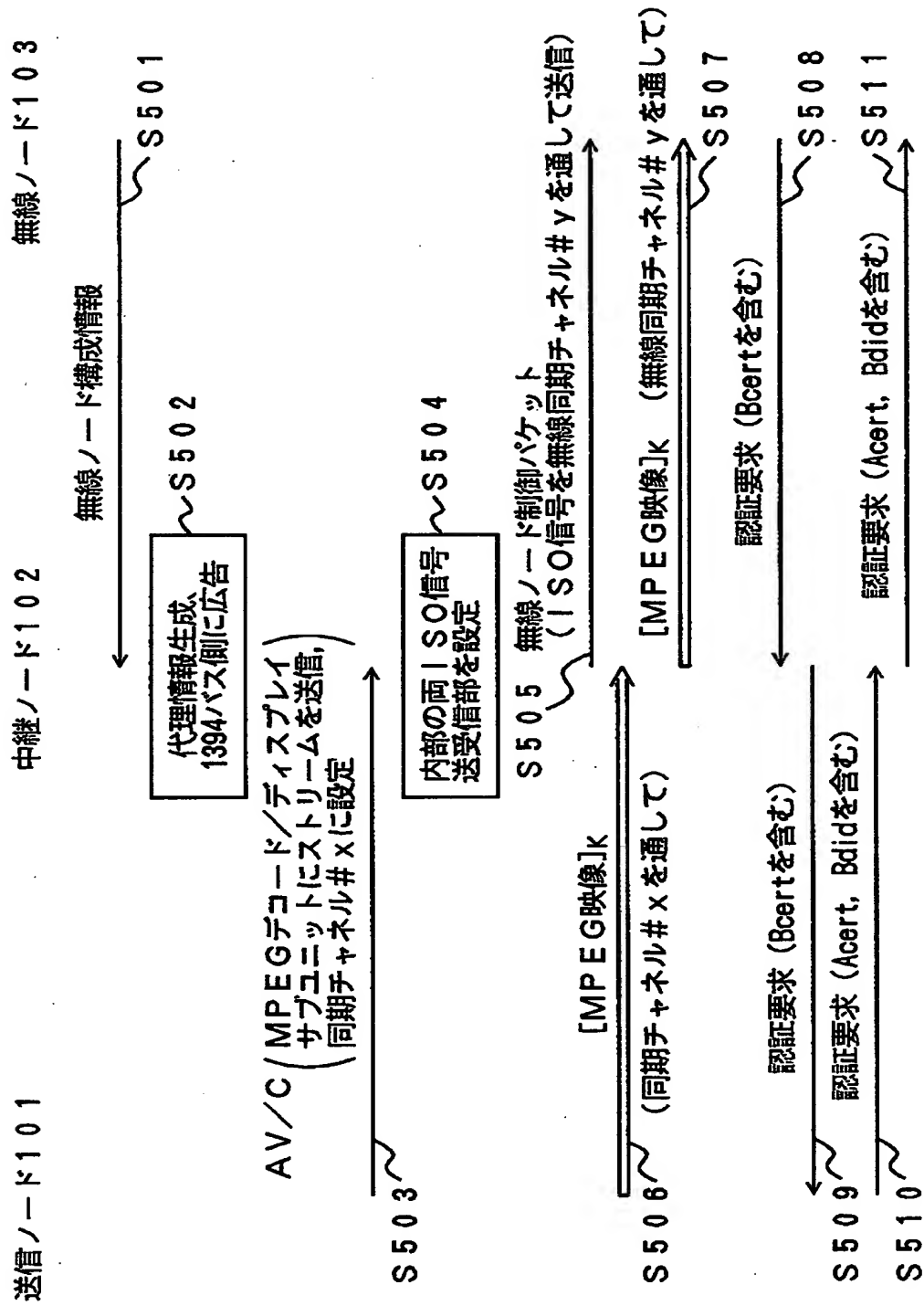
【図 3】



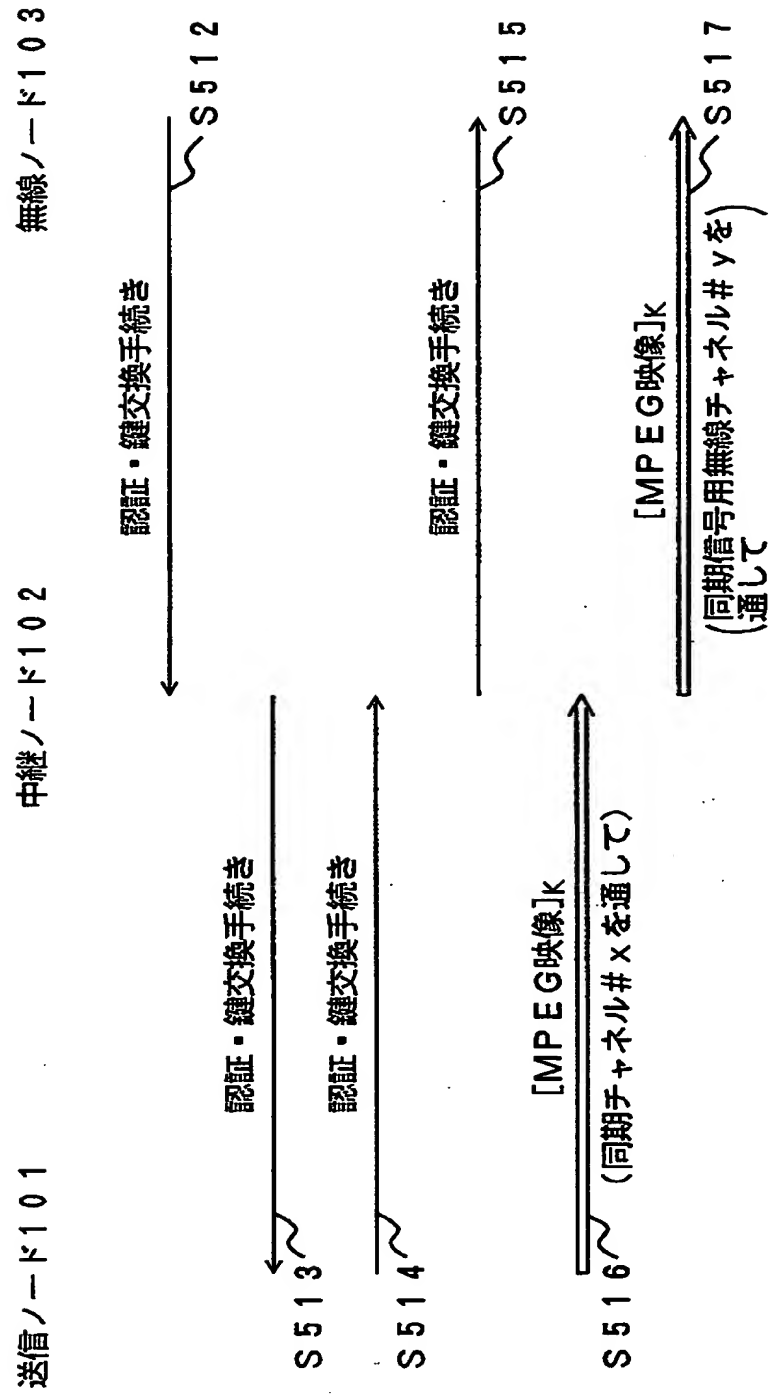
【図 4】



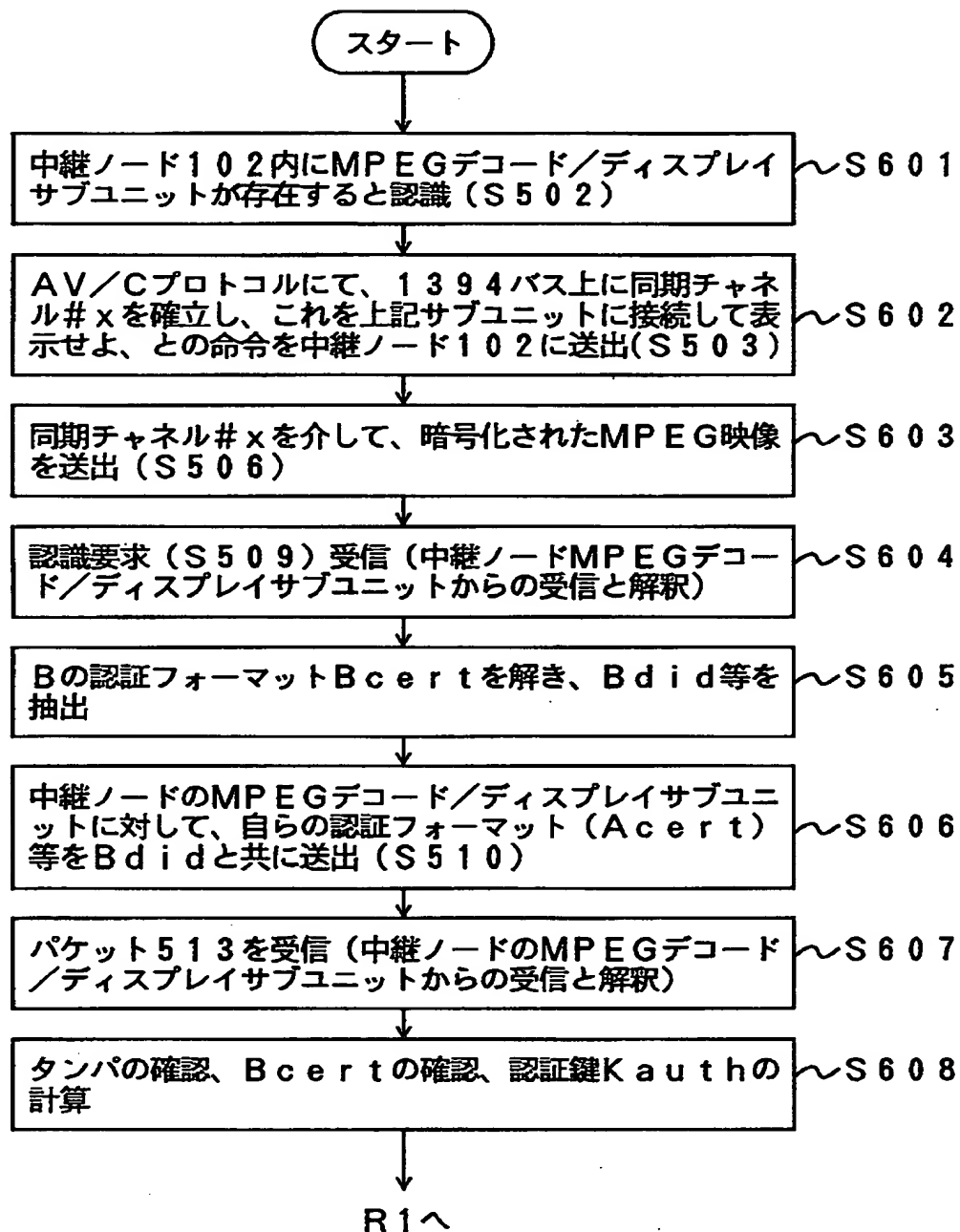
【図 5】



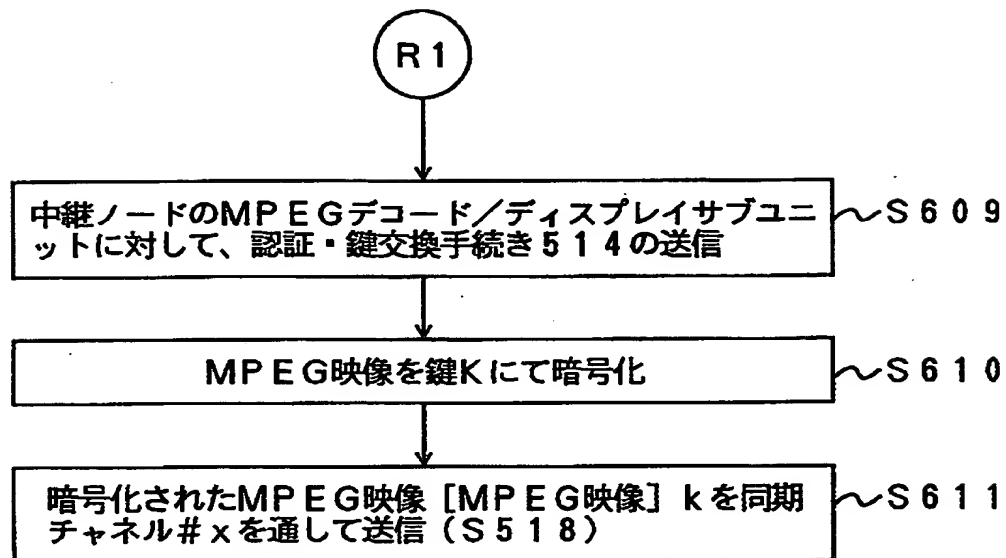
【図 6】



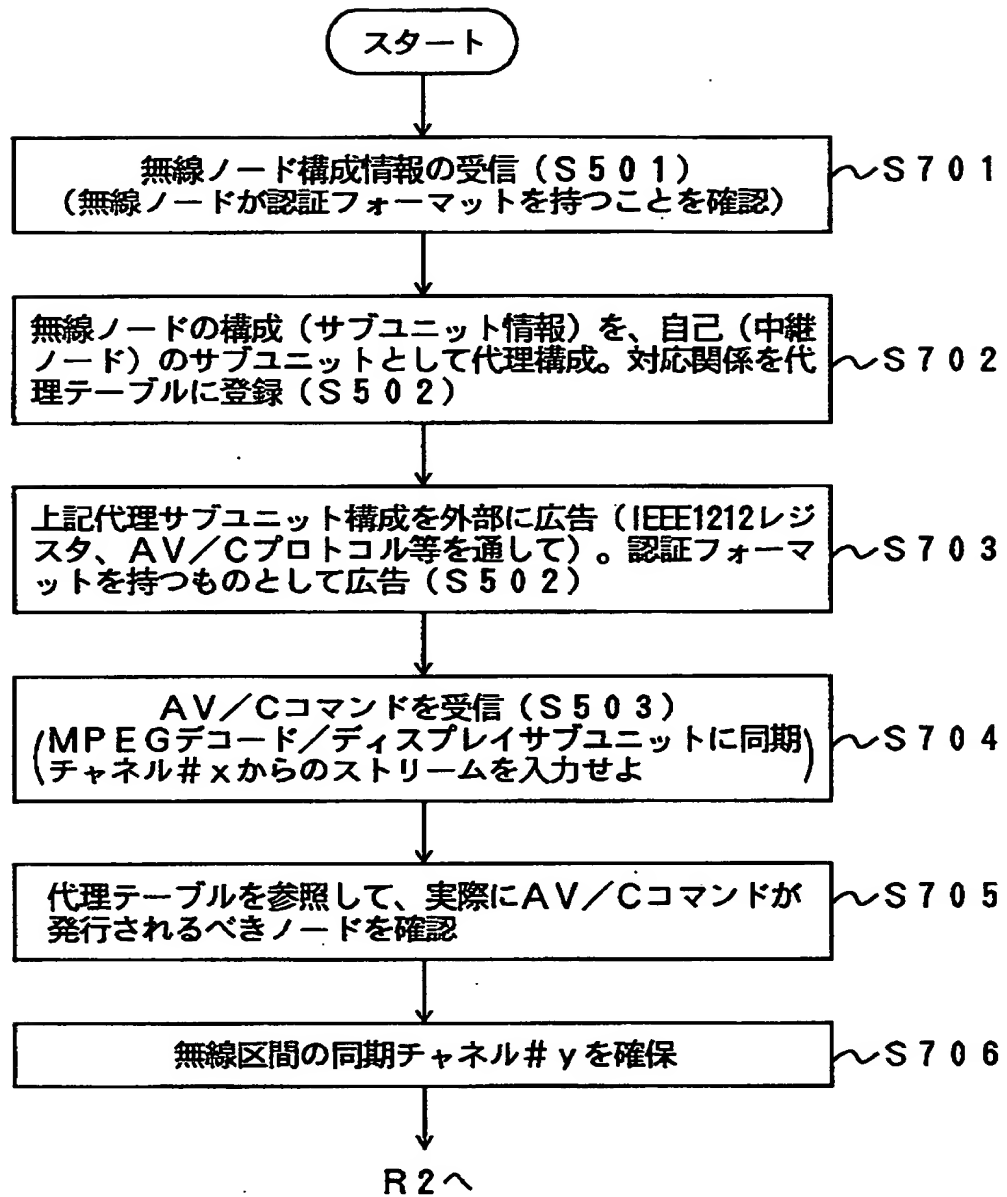
【図 7】



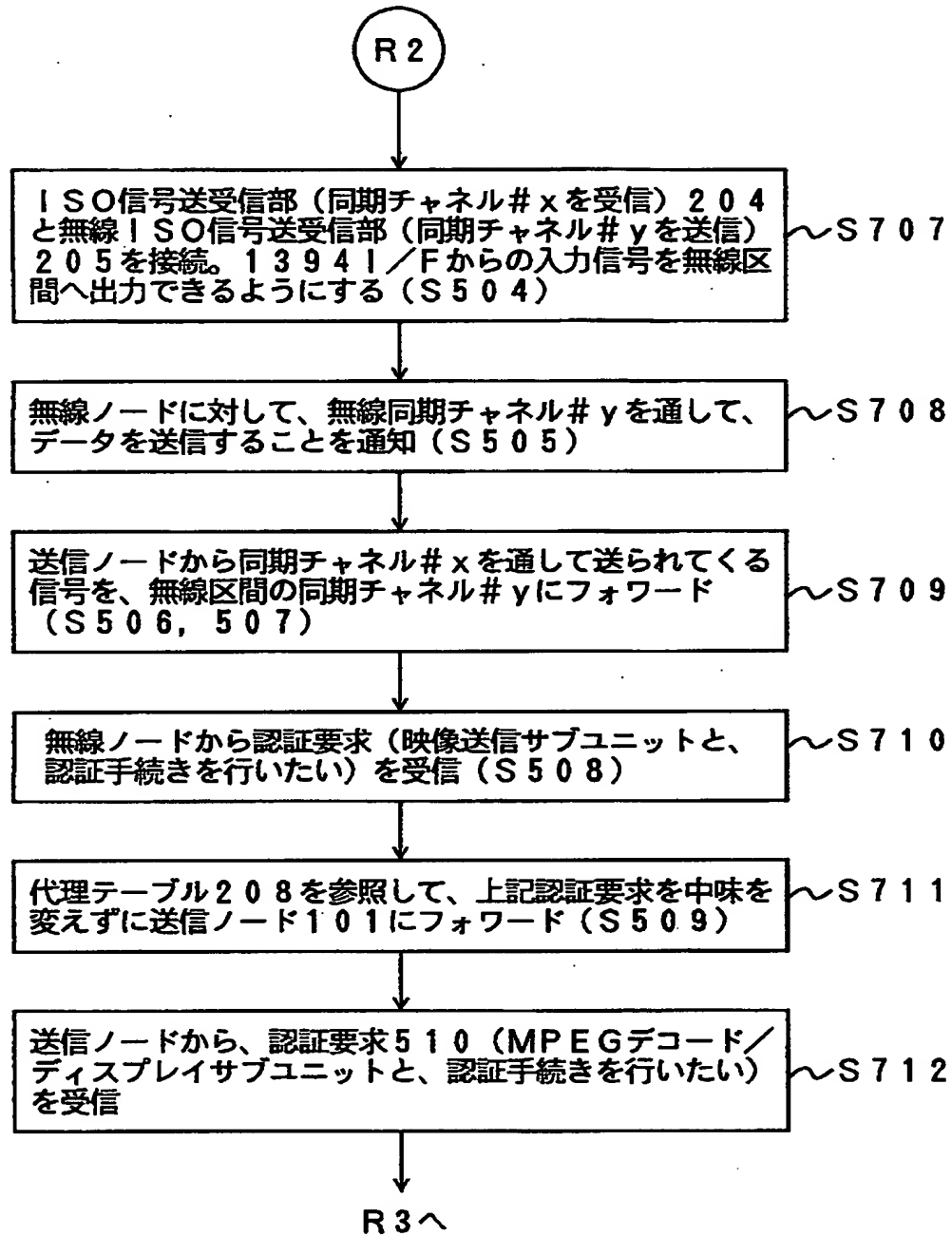
【図 8】



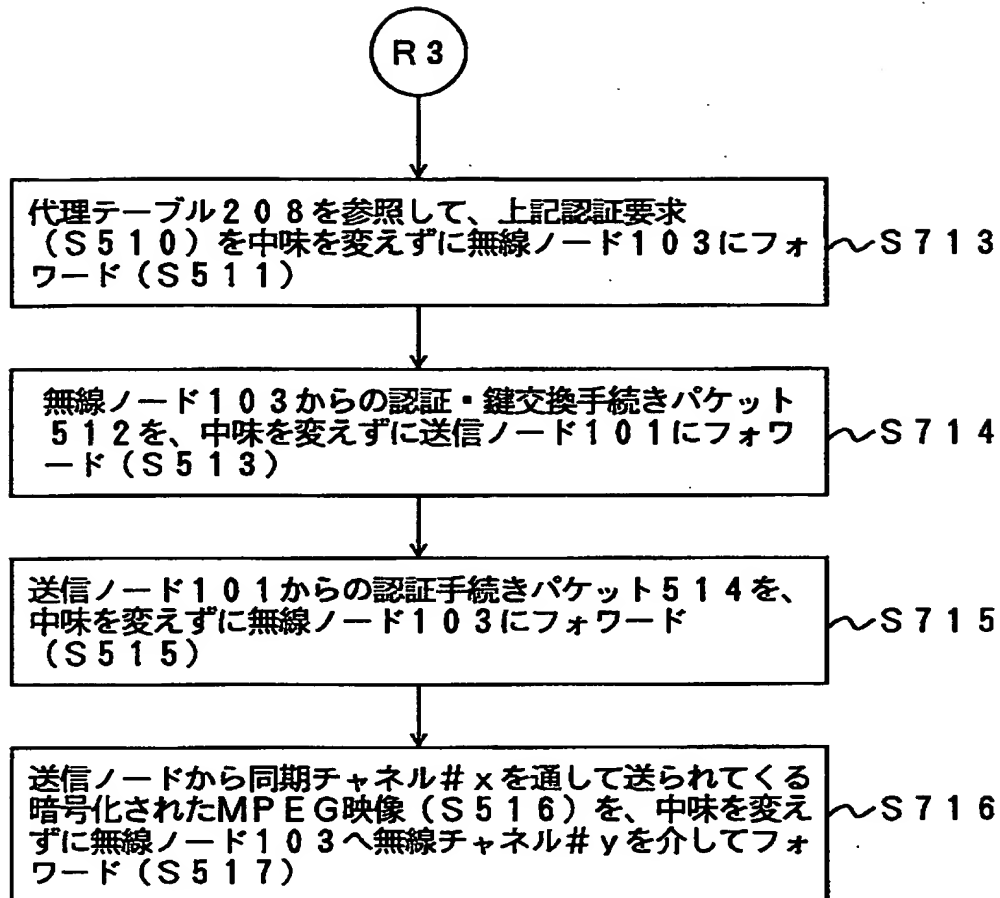
【図 9】



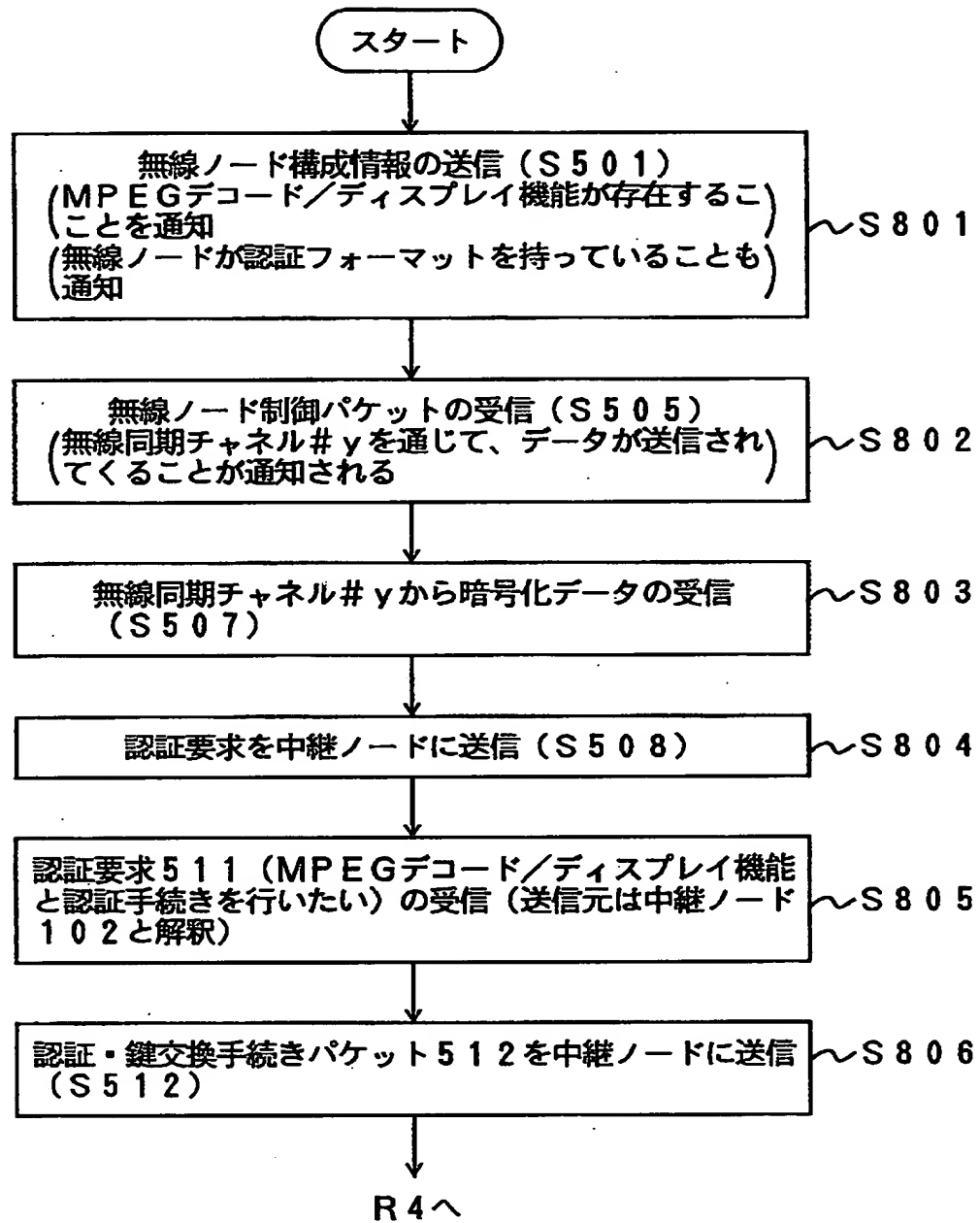
【図 10】



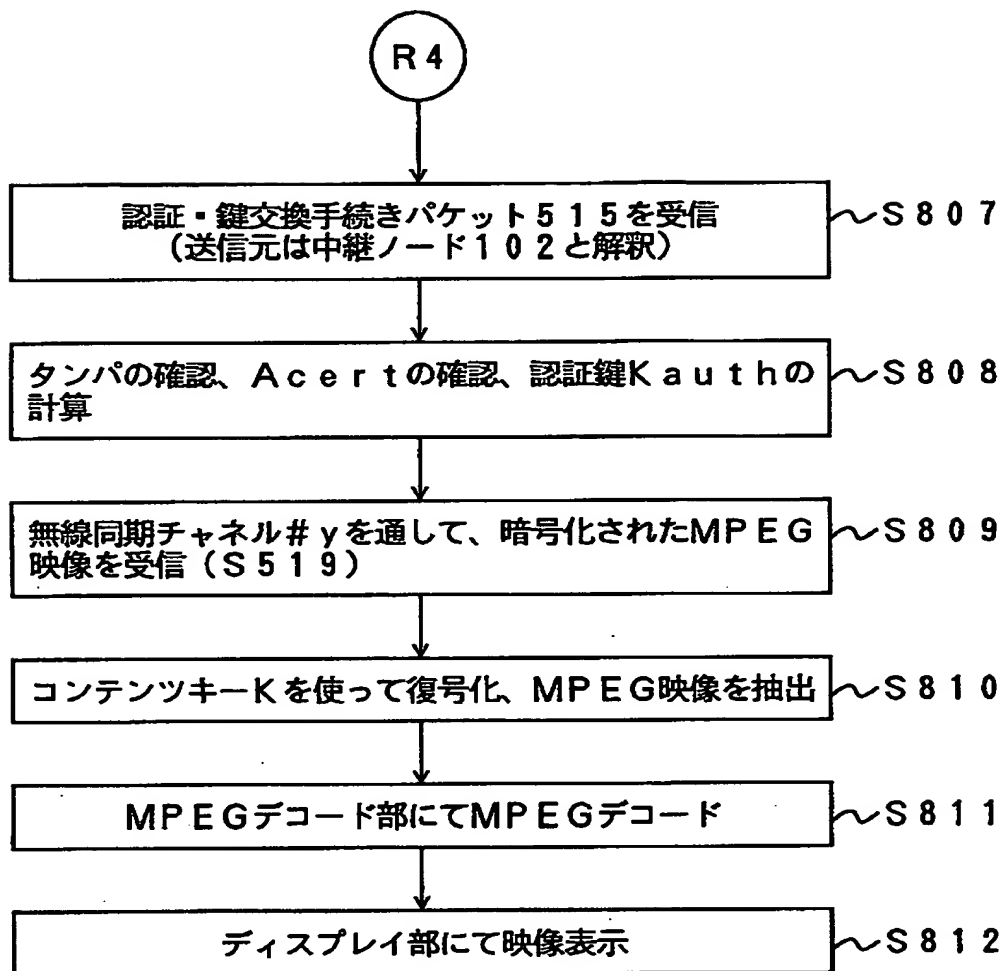
【図 11】



【図 12】



【図 13】



【図 14】

宛先ノード=中継ノード
送信元ノード=無線ノード
構成1=MPEGデコード/ディスプレイ機能
構成2= ...
⋮
構成1の属性1=認証フォーマット (認証機関=...)
構成1の属性2=MPEGの上限ビットレート6Mbps
⋮

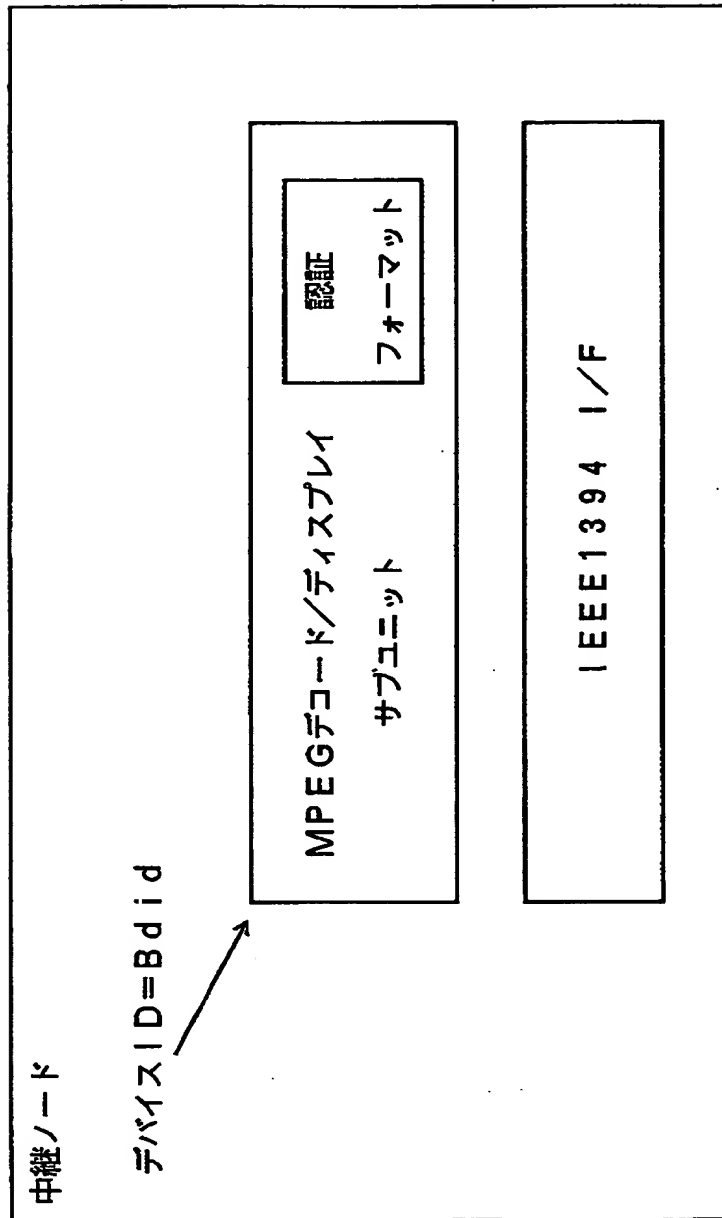
【図 15】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード103の MPEGデコード/ディスプレイ機能 (認証フォーマット有)	MPEGデコード/ディスプレイサブユニット (認証フォーマット有)
.....	.....

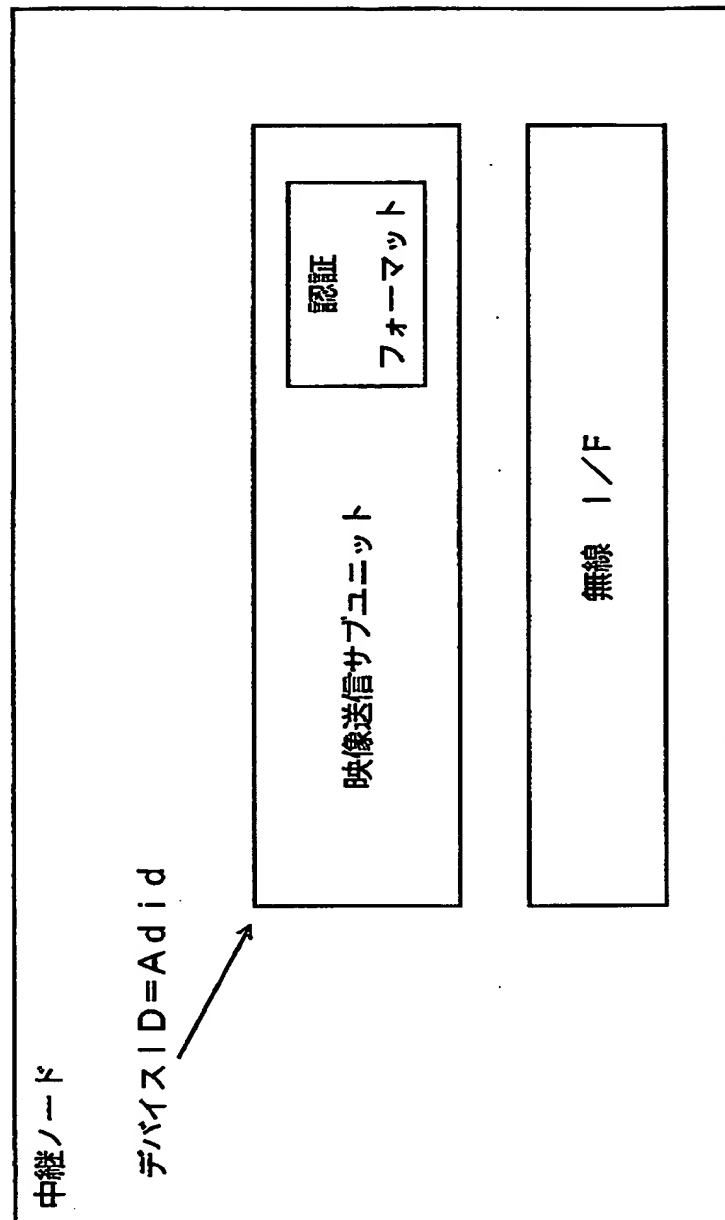
【図 16】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード101の映像送信機能 (映像送信サブユニット) (認証フォーマット有)	映像送信サブユニット (認証フォーマット有)
.....	.....

【図 17】



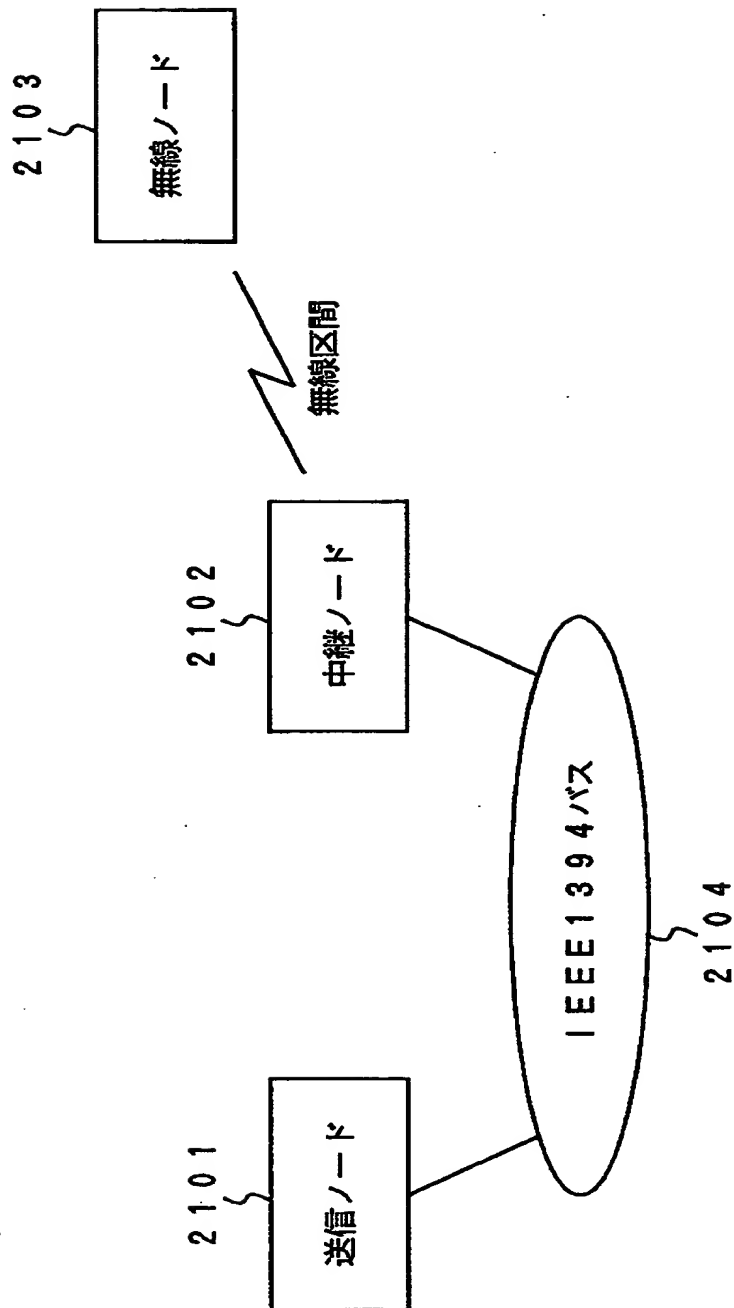
【図 18】



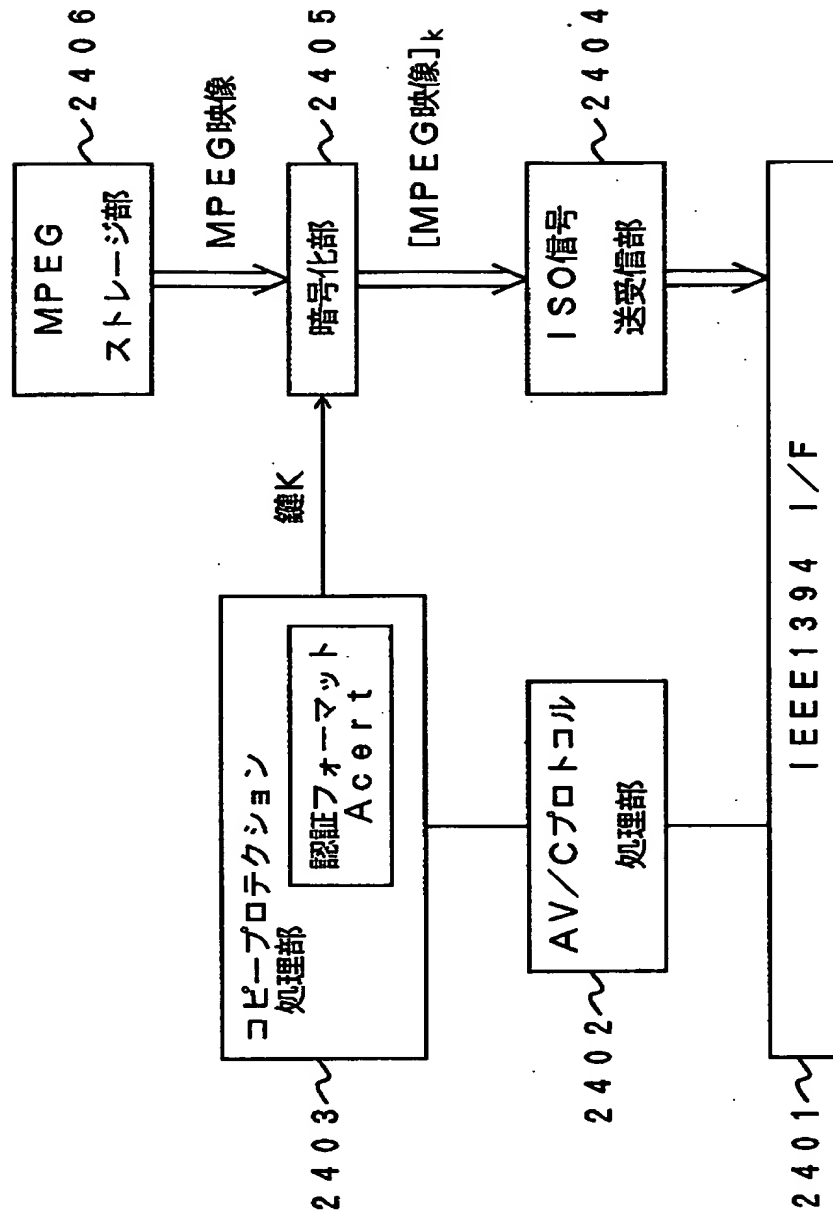
【図 1 9】

宛先ノード=無線ノード
送信元ノード=中継ノード
制御内容=データ受信
使用無線同期チャネル=# y
データ送信先=MPEGデコード/ディスプレイ機能
データ送信元=映像送信機能
⋮

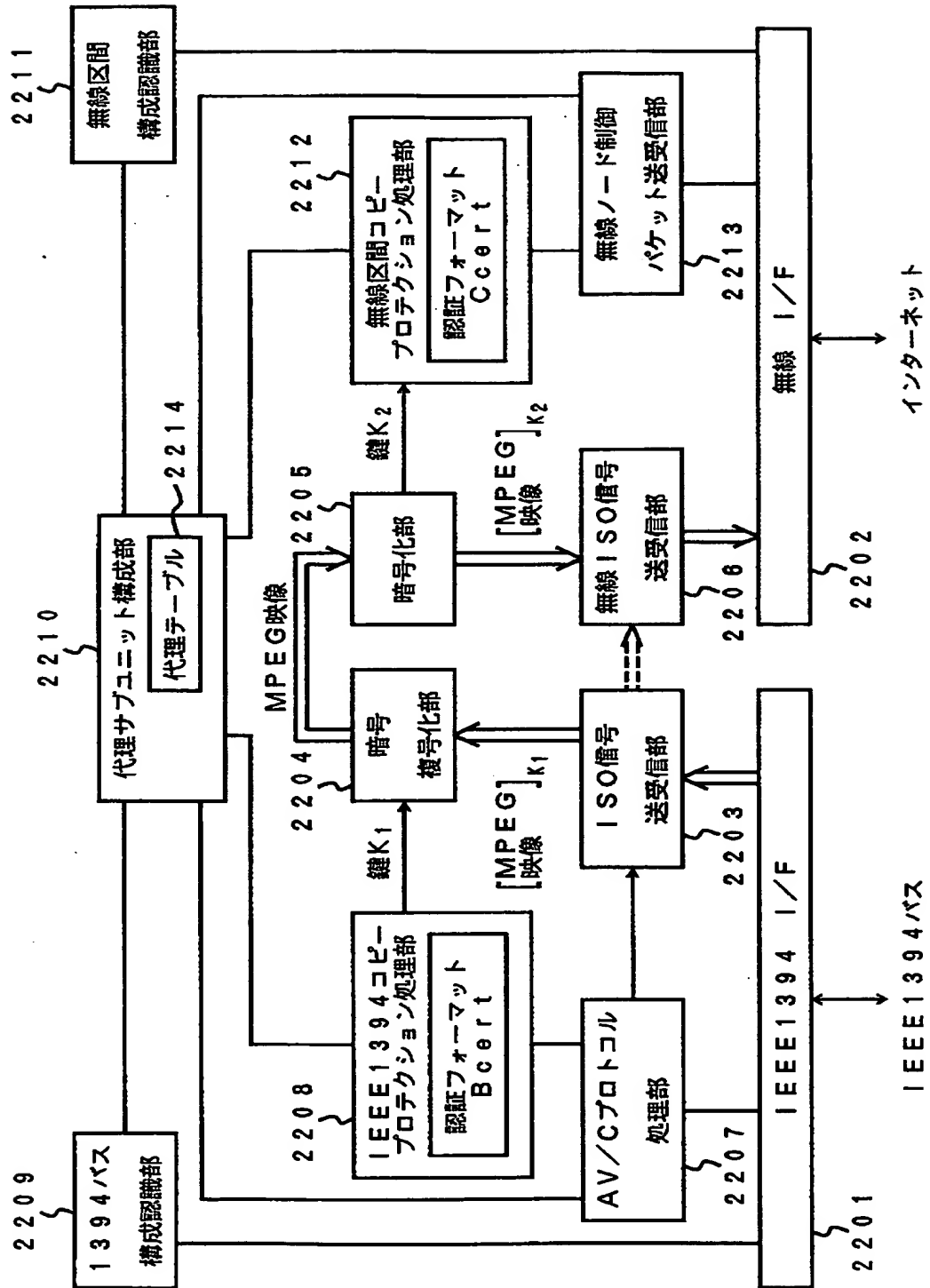
【図 20】



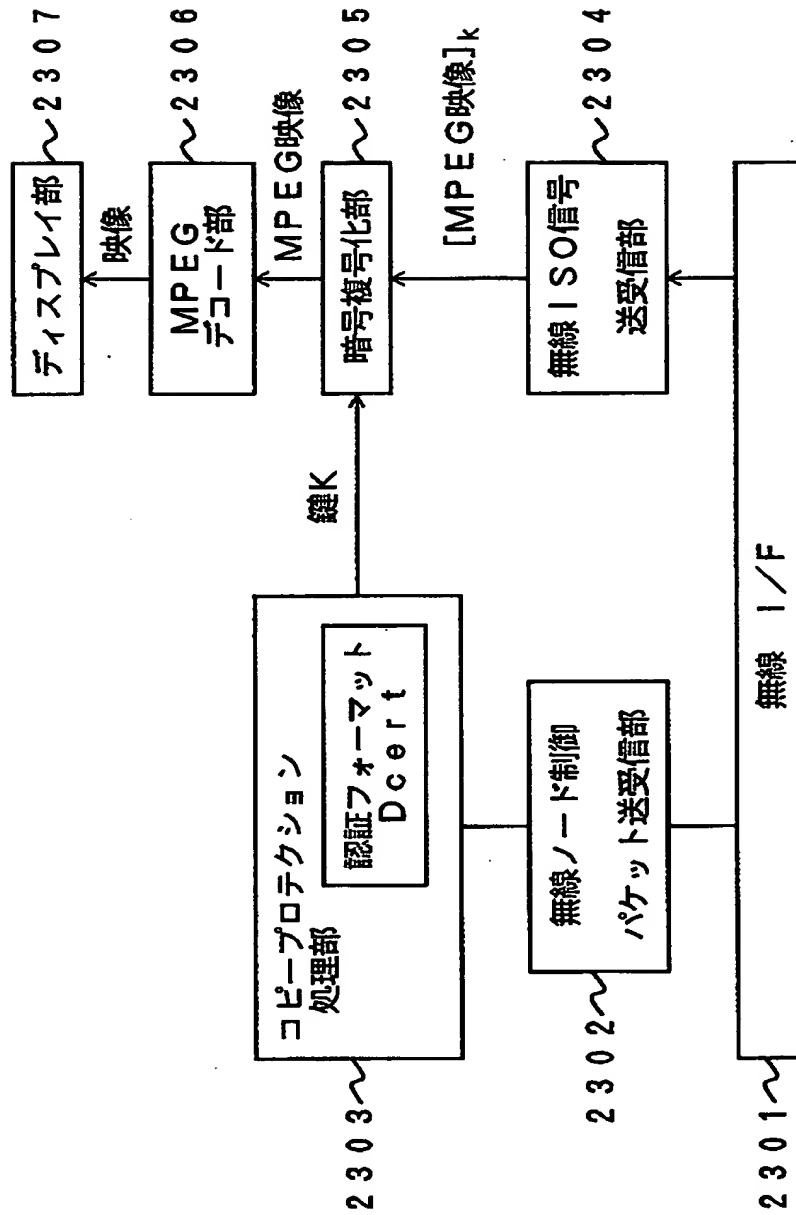
【図 21】



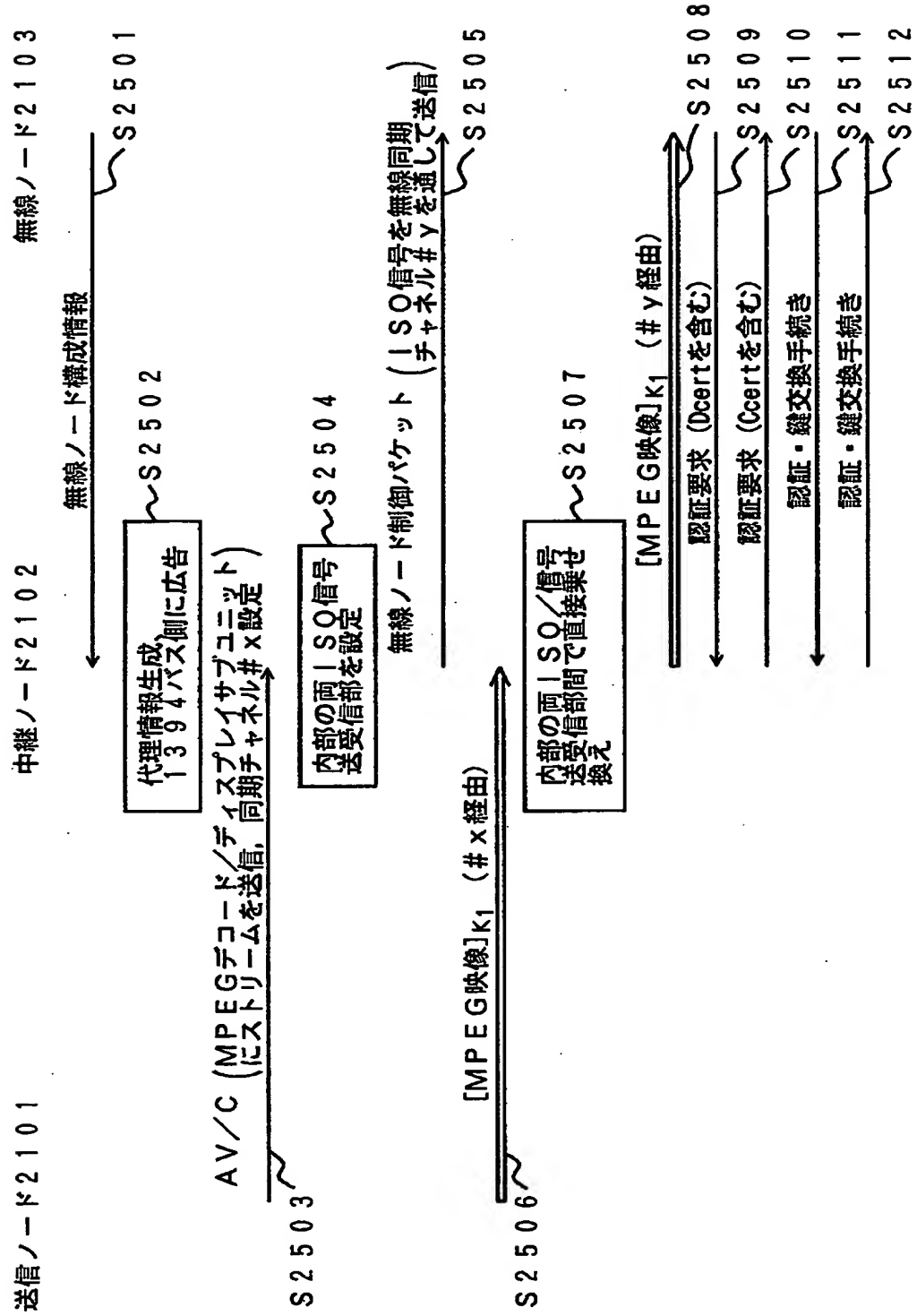
【図 22】



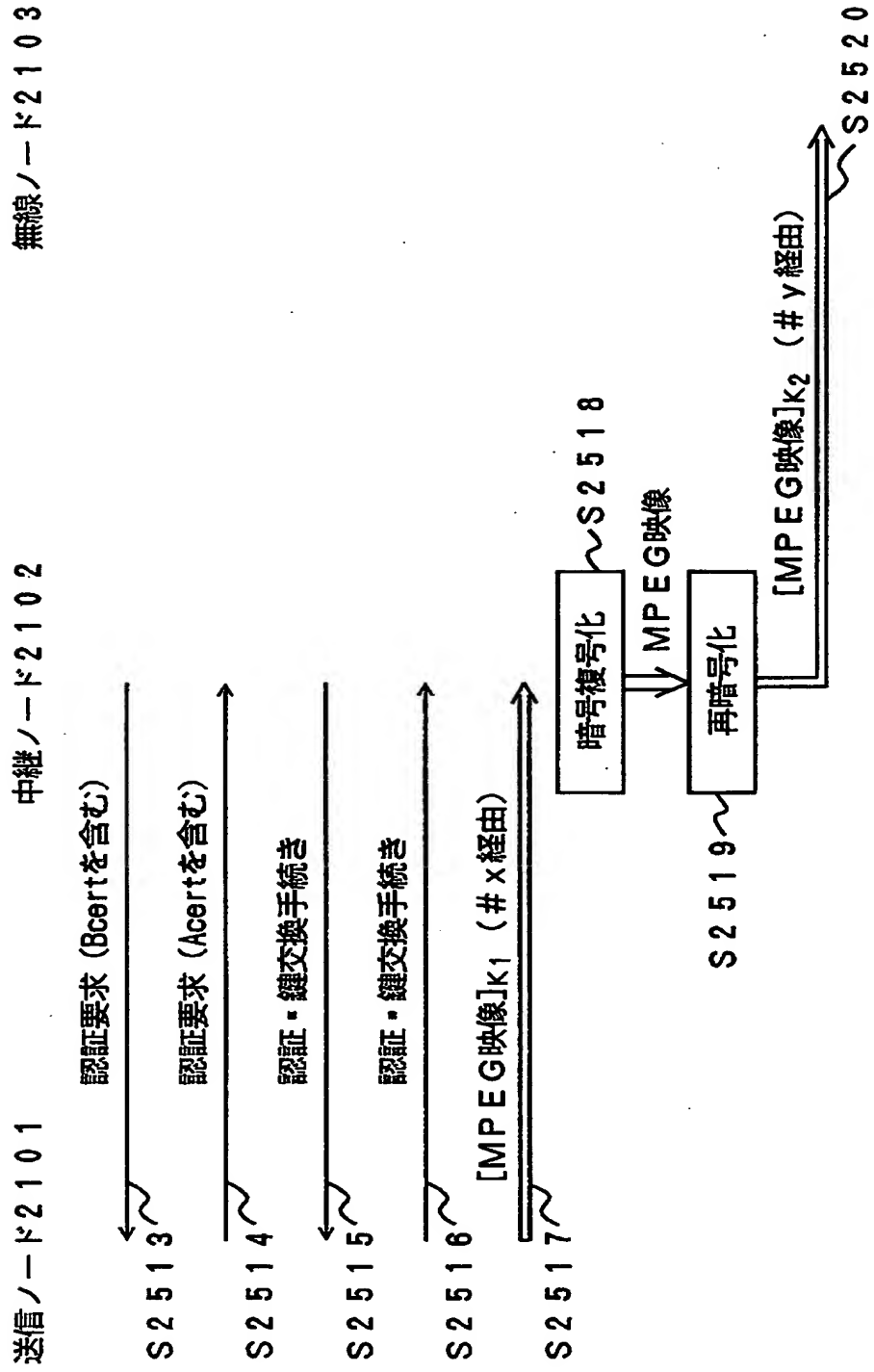
【図 23】



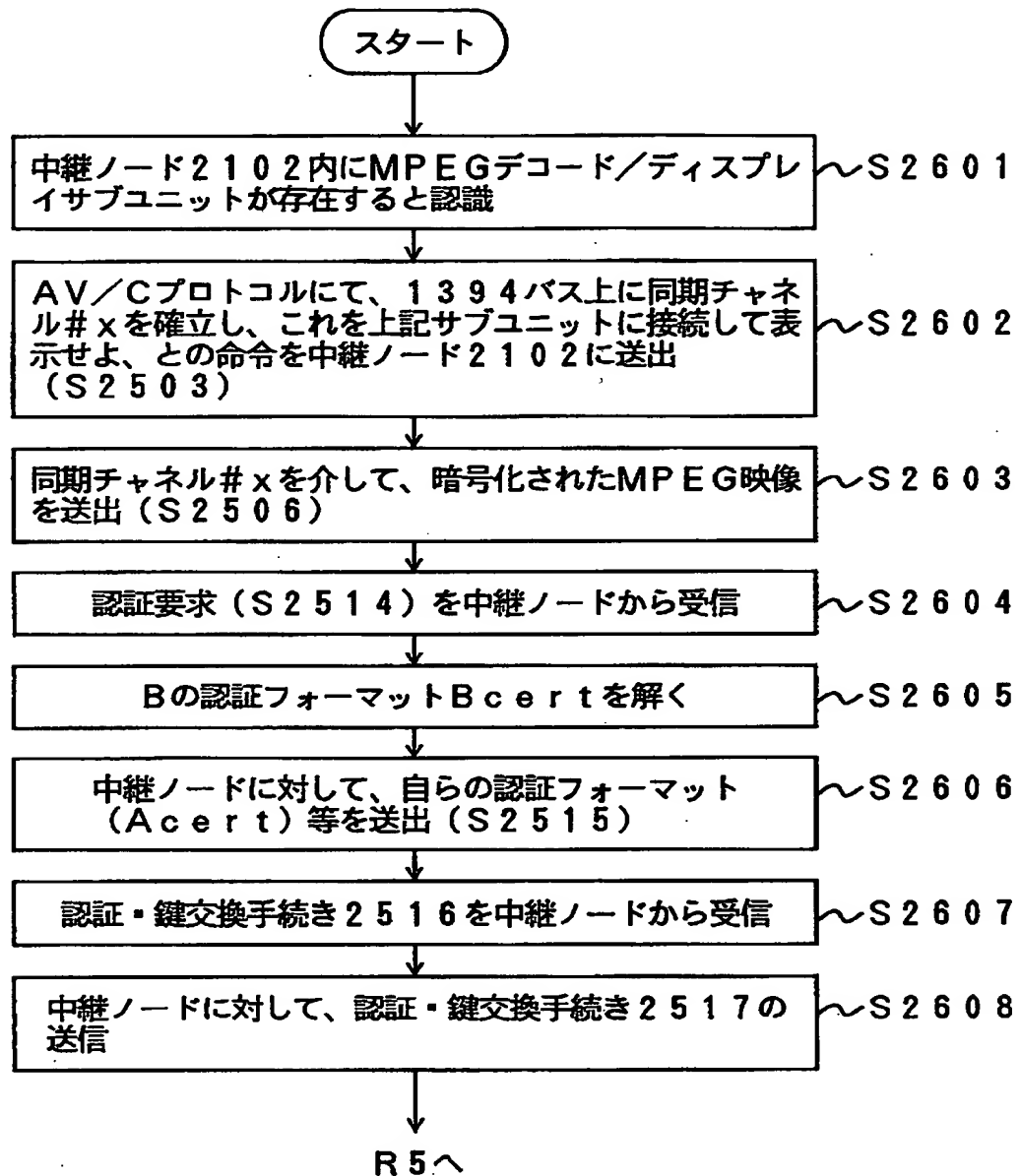
【図 24】



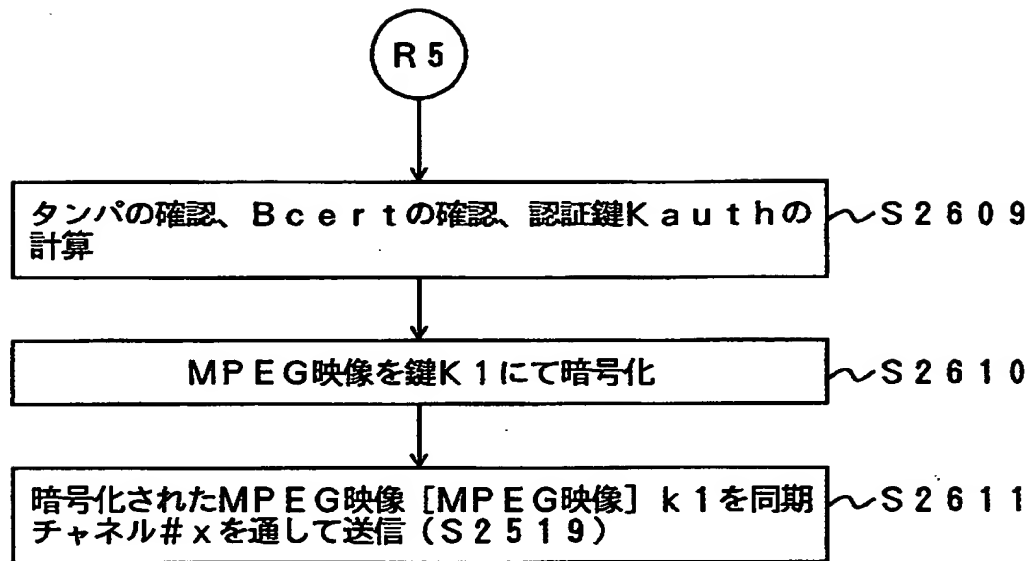
【図 25】



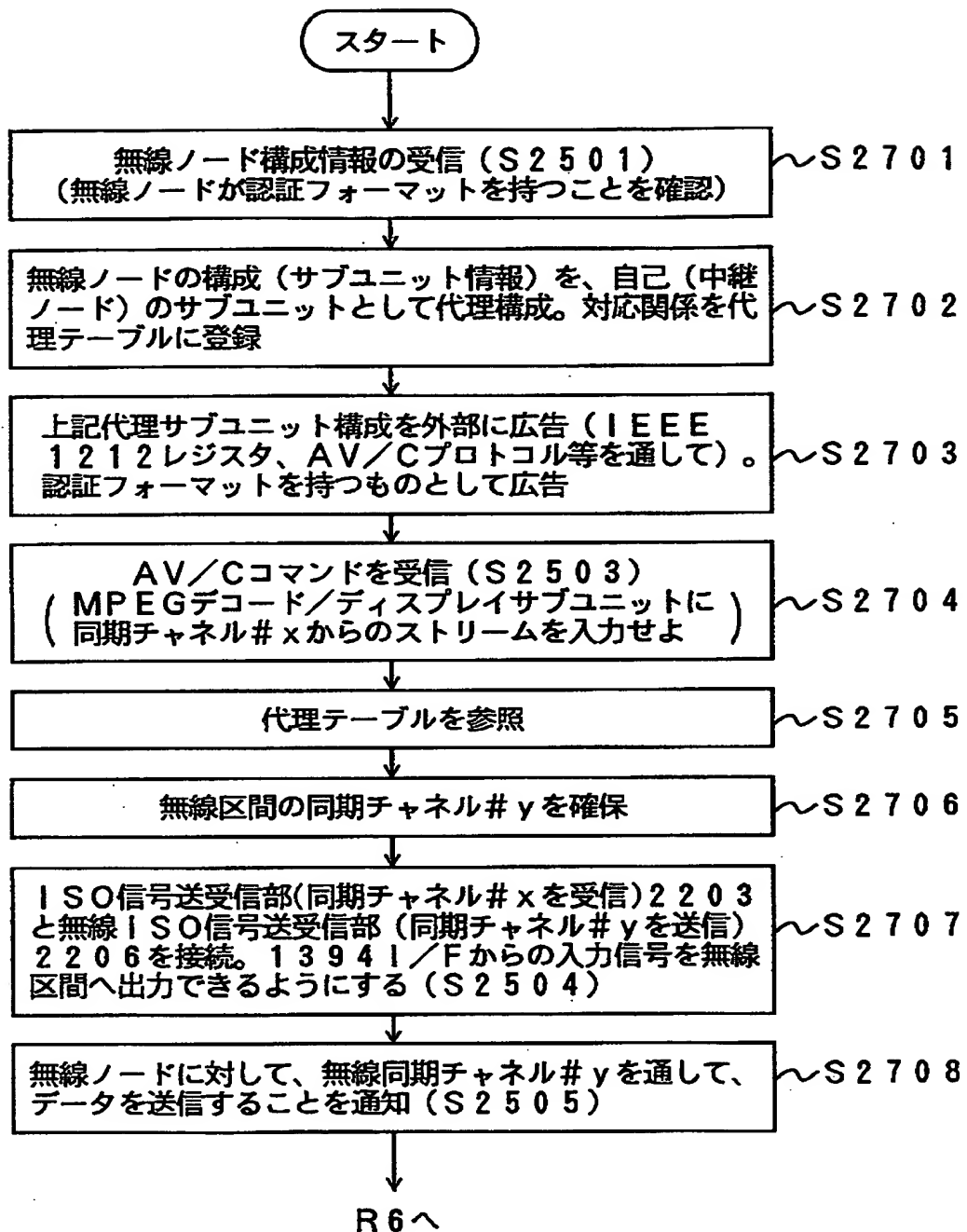
【図 26】



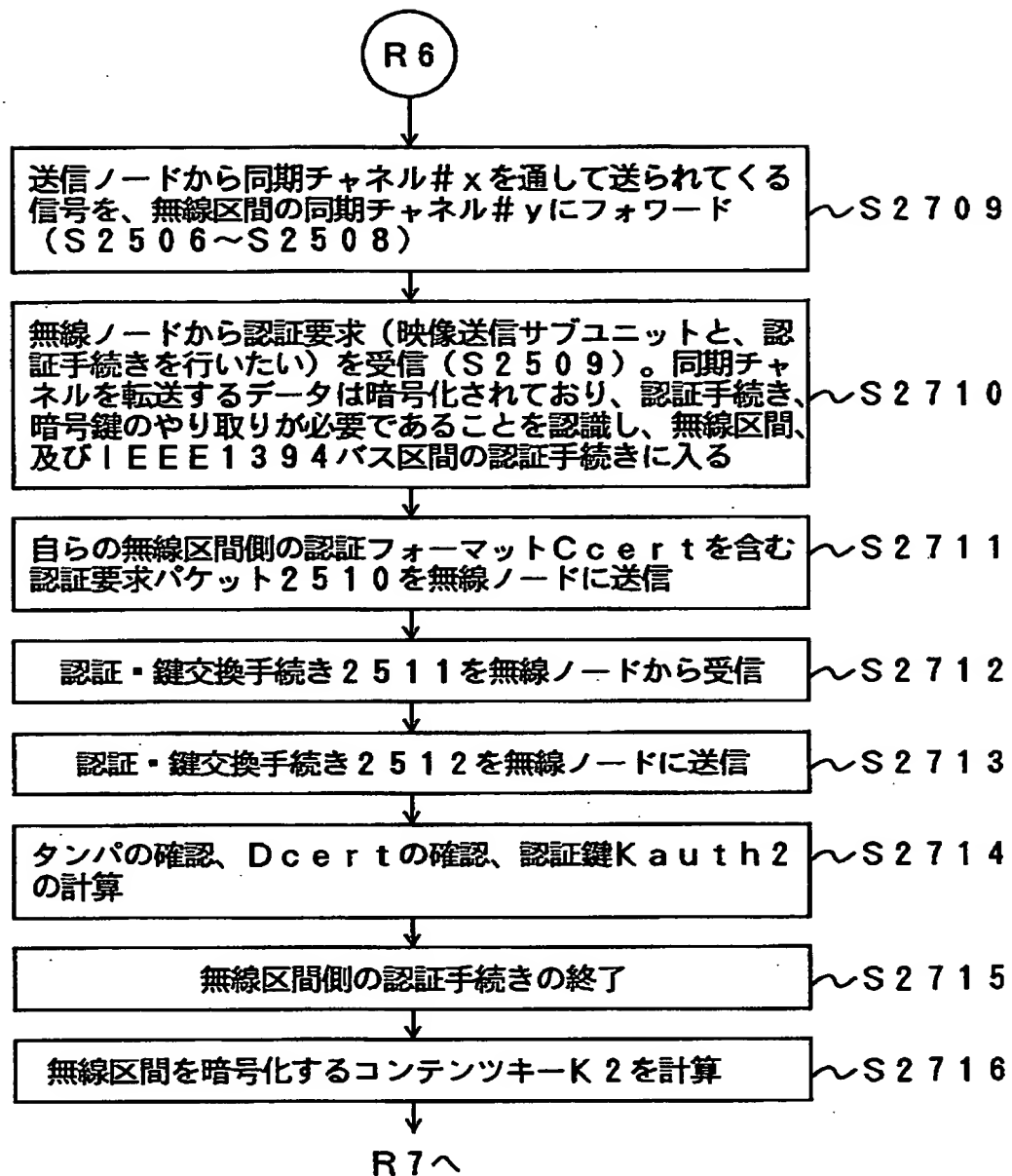
【図 27】



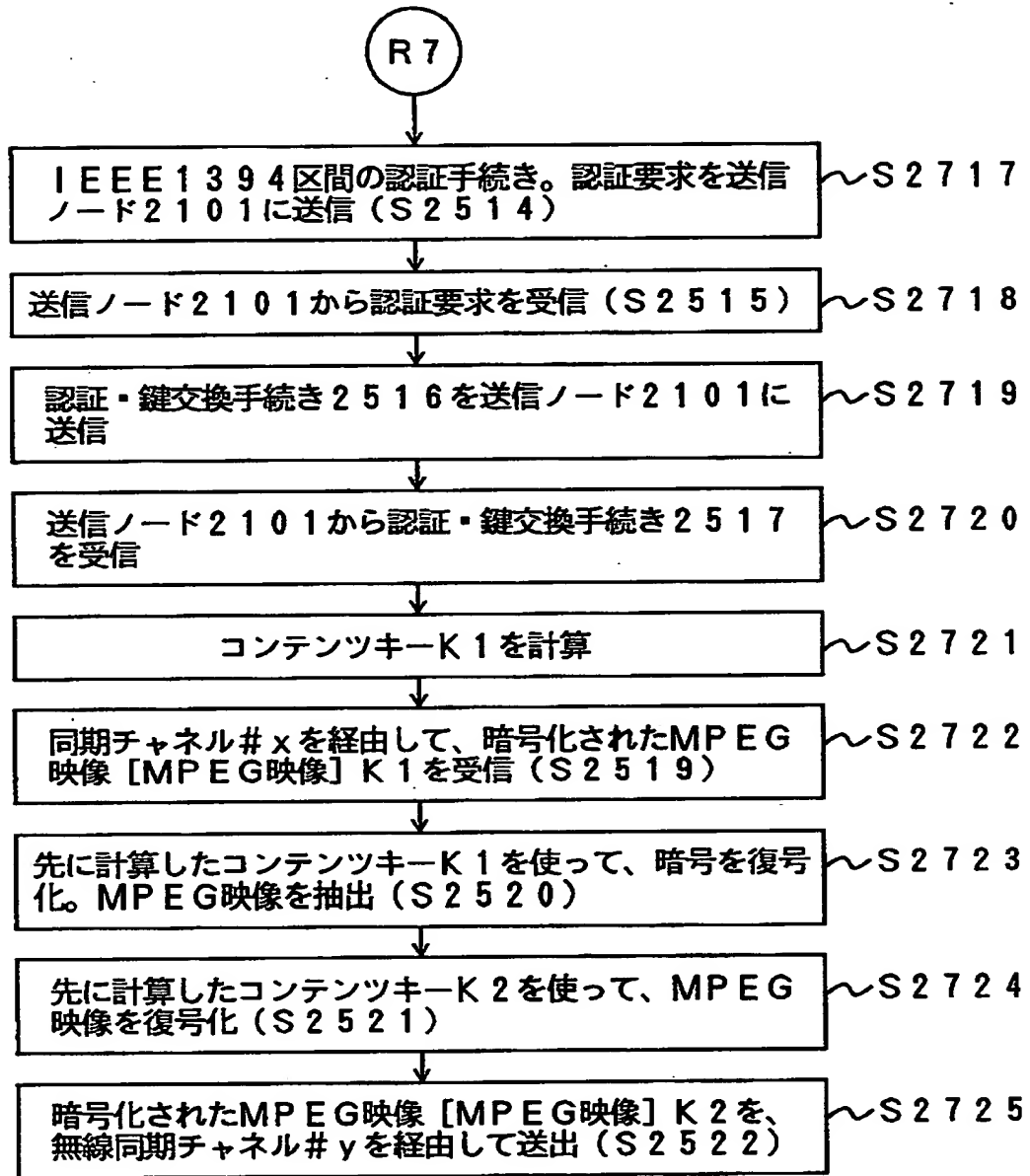
【図 28】



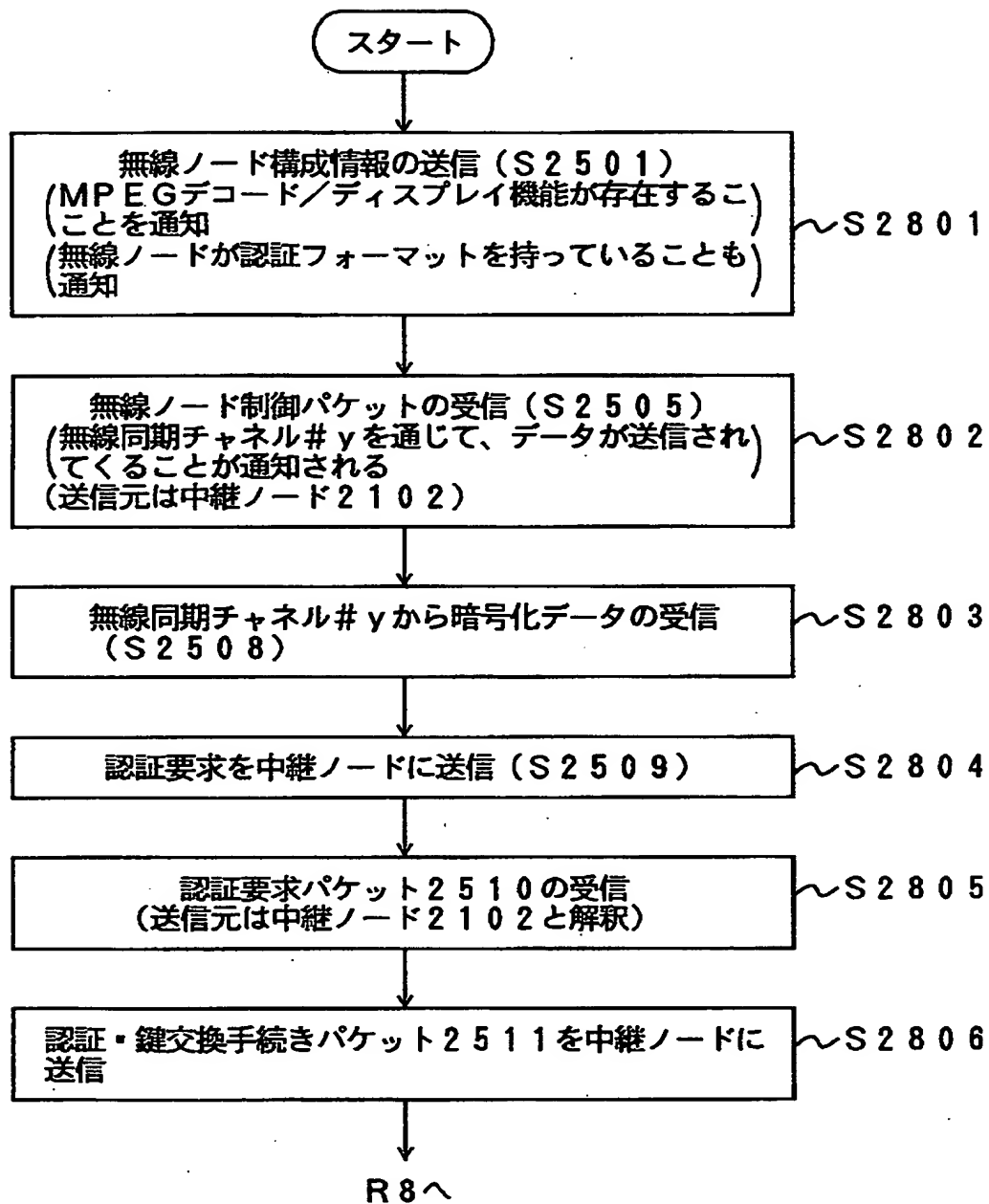
【図 29】



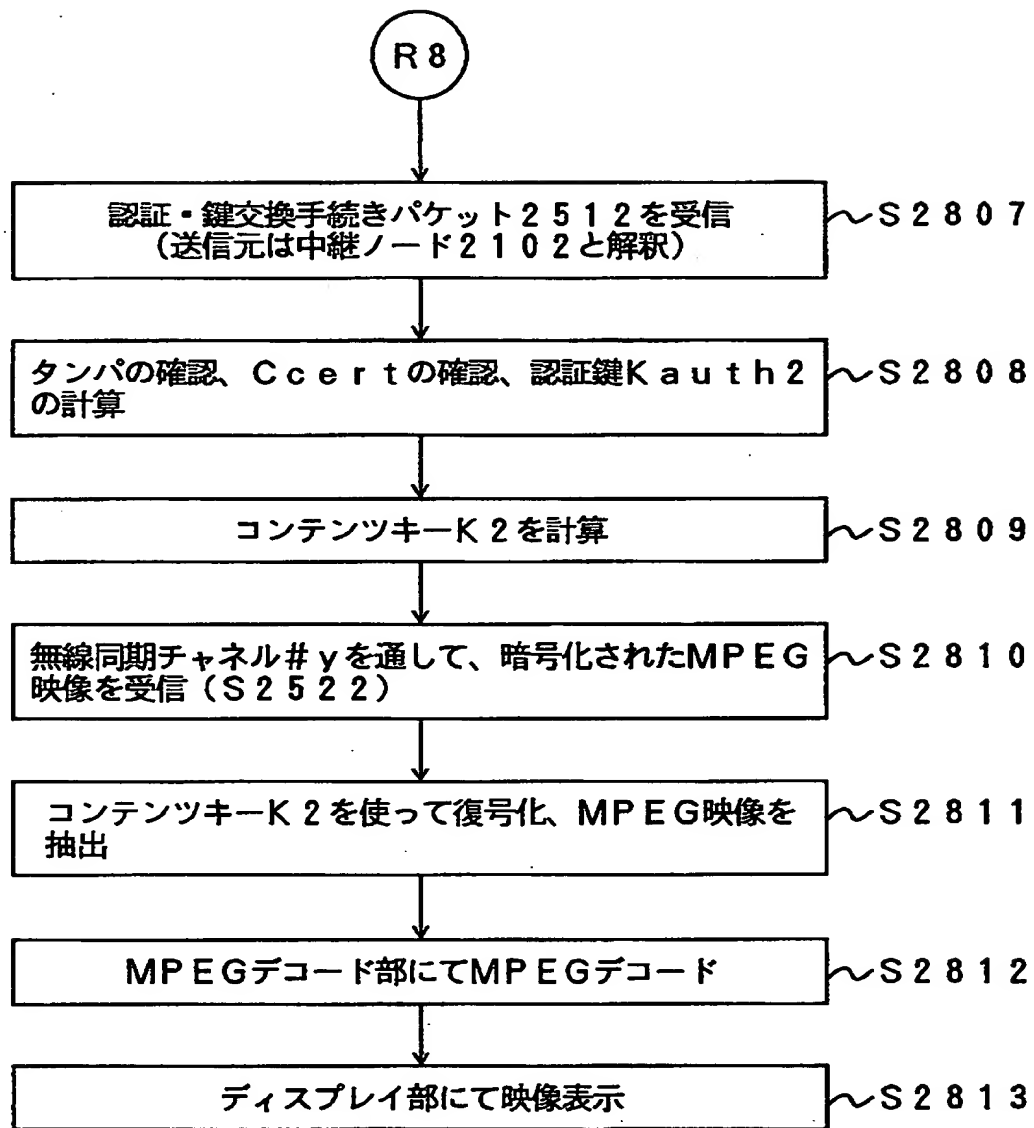
【図 30】



【図 31】



【図 3 2】



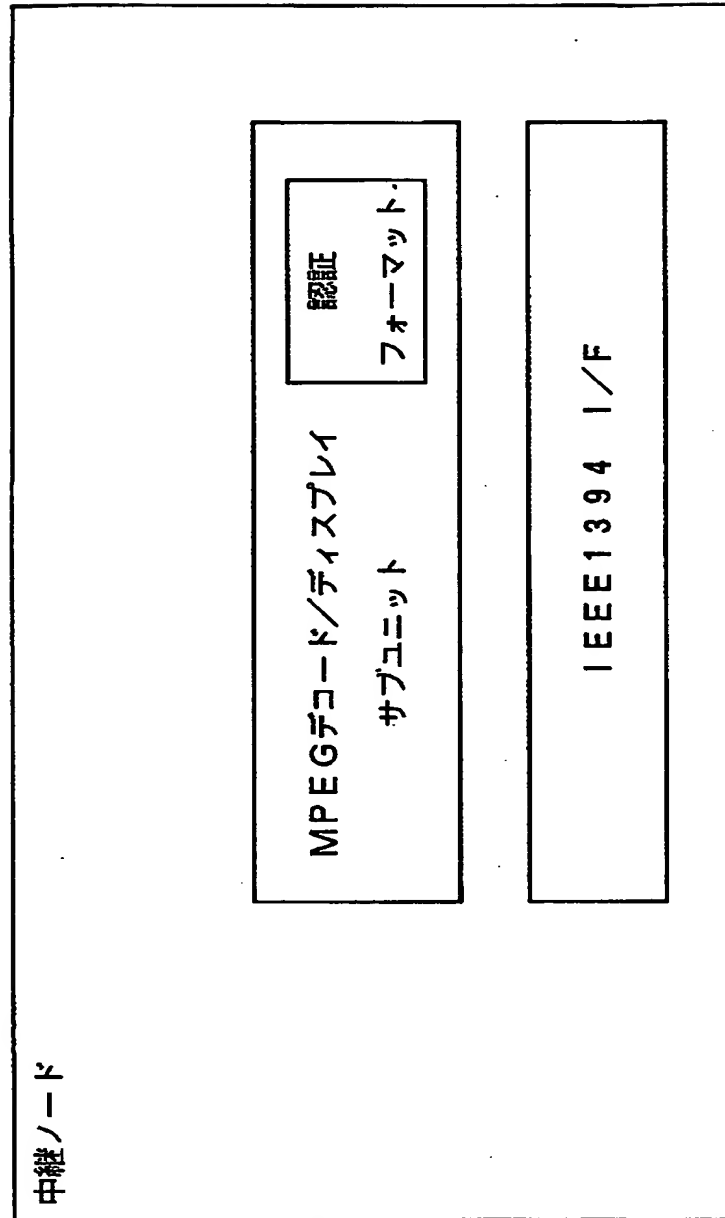
【図 33】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード103の MPEGデコード/ディスプレイ機能	MPEGデコード/ディスプレイサブユニット
...	...

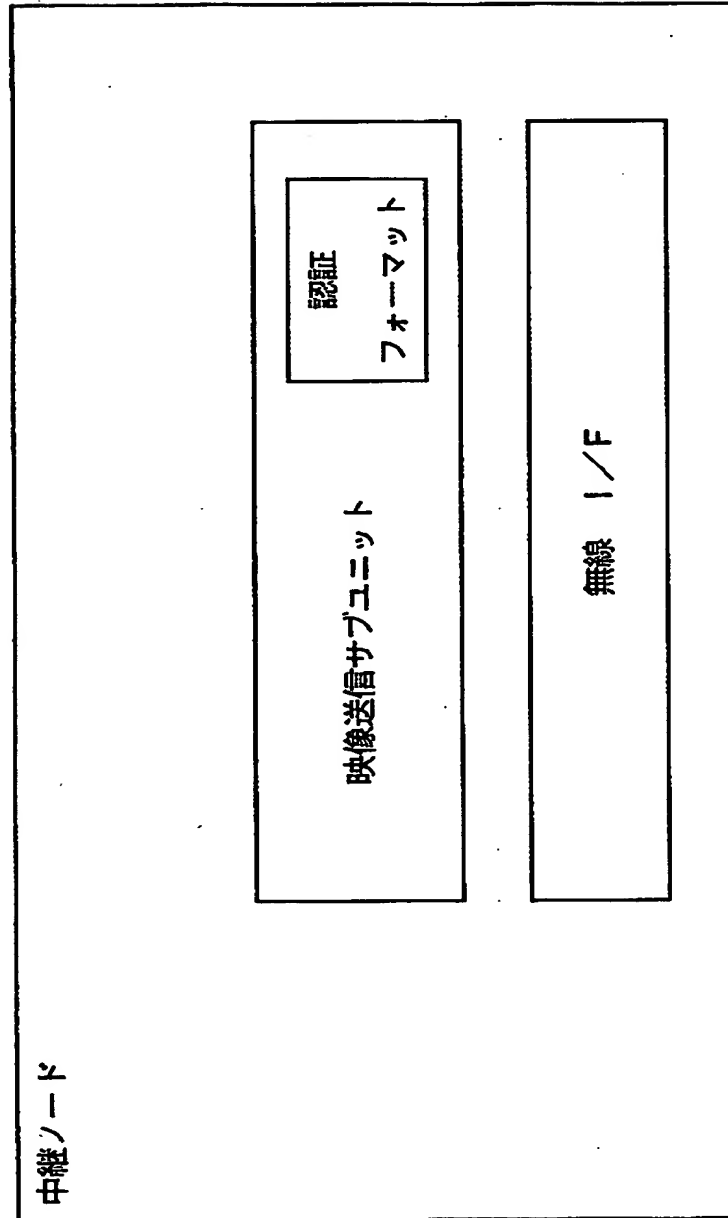
【図 34】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード101の映像送信機能 (映像送信サブユニット)	映像送信サブユニット
...	...

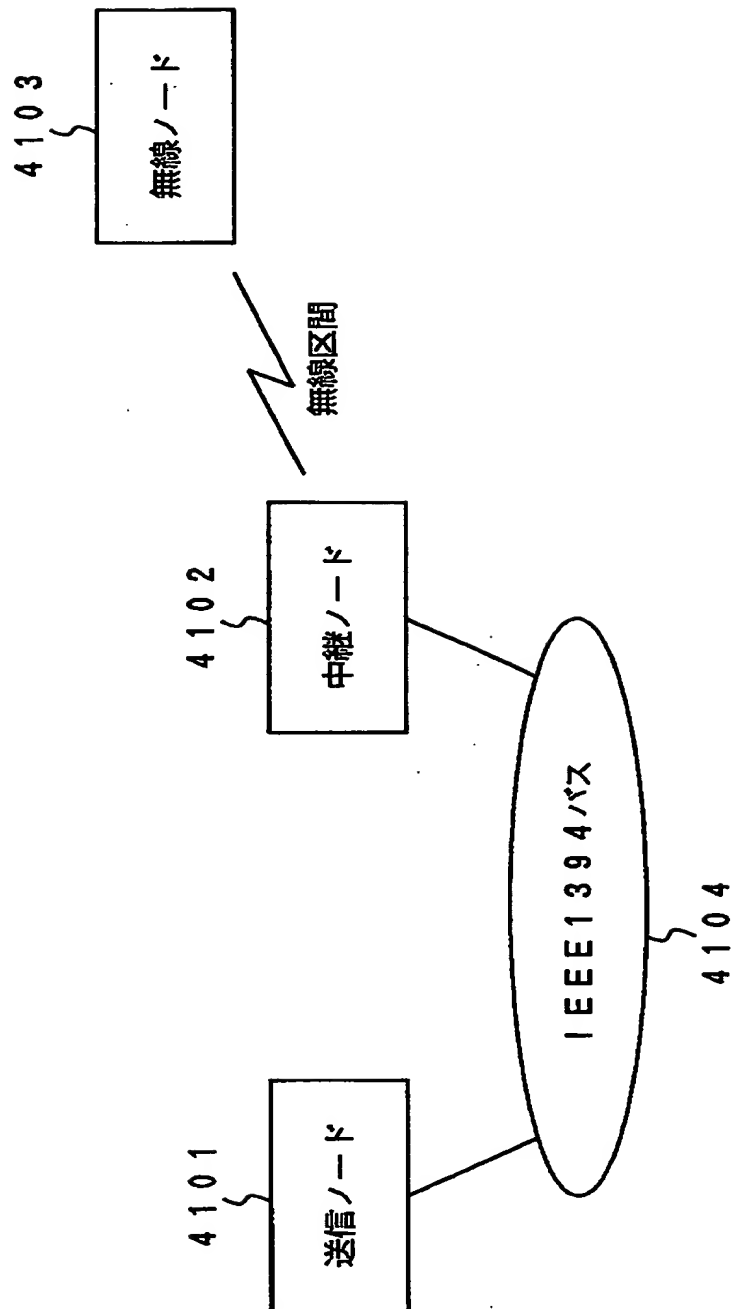
【図 35】



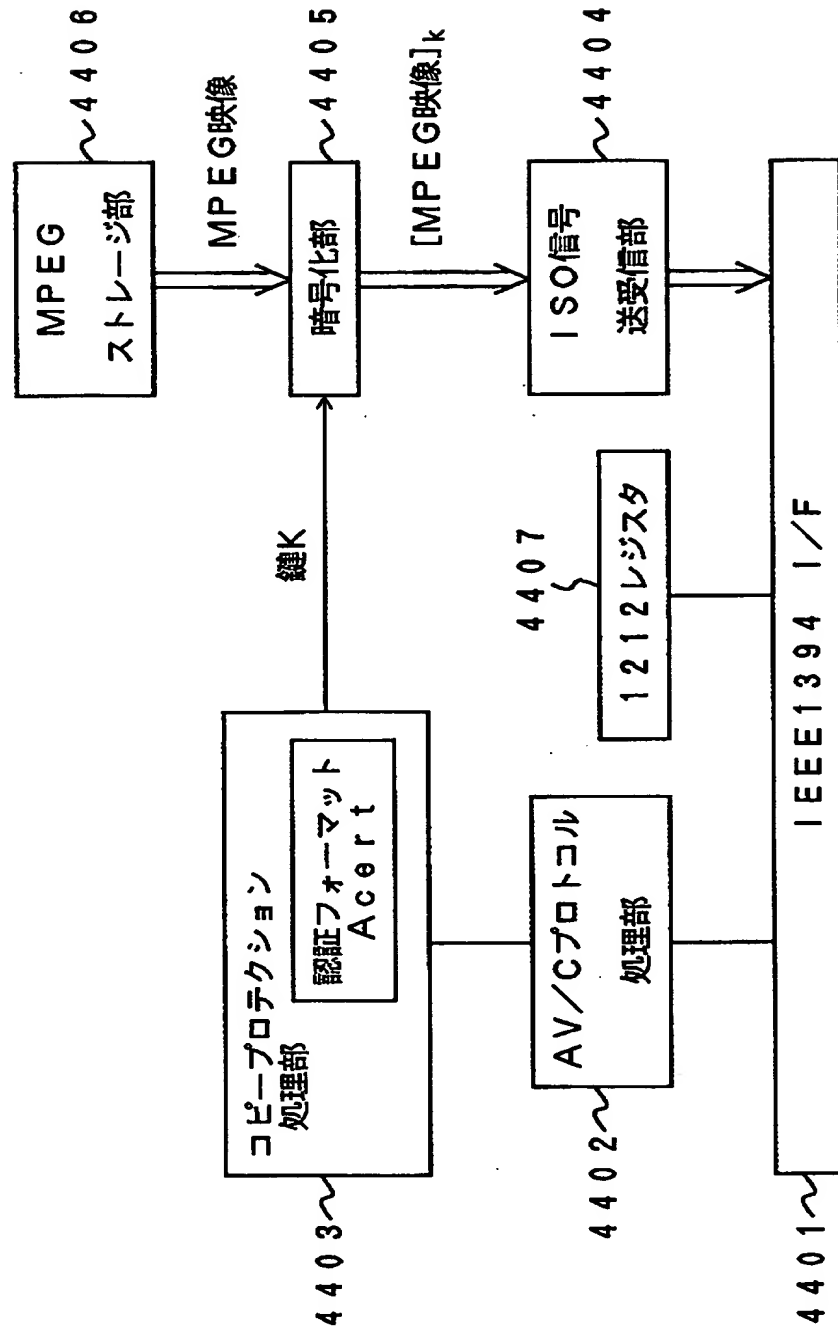
【図 36】



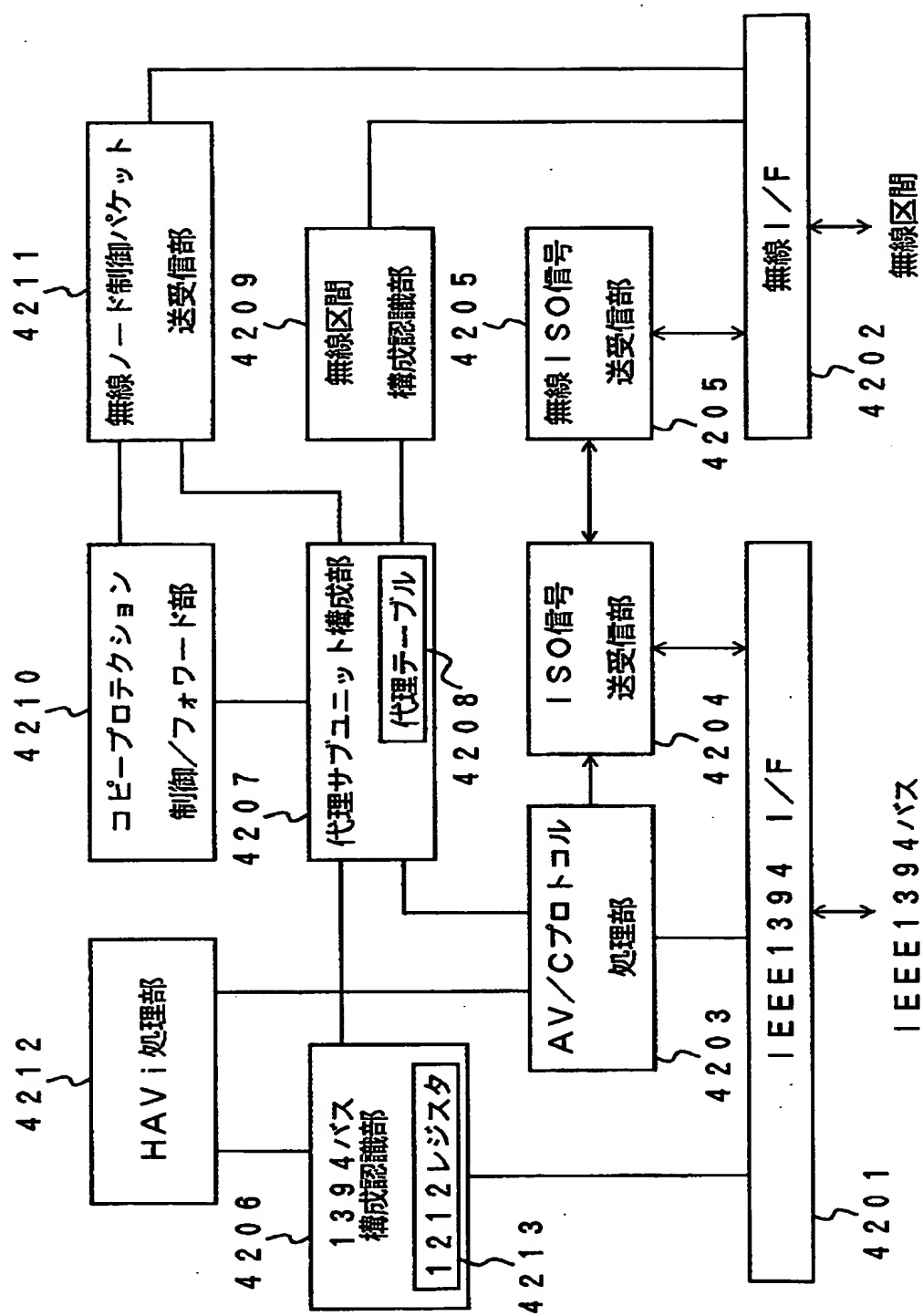
【図 37】



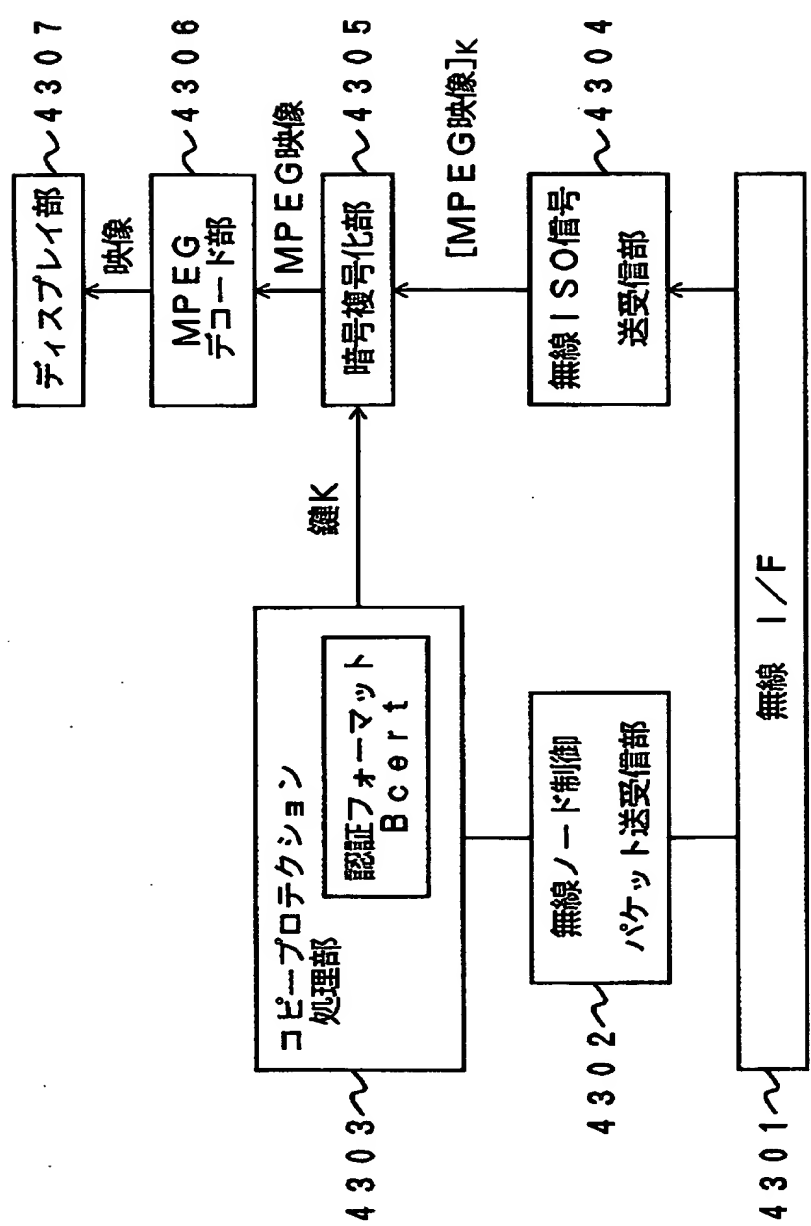
【図 38】



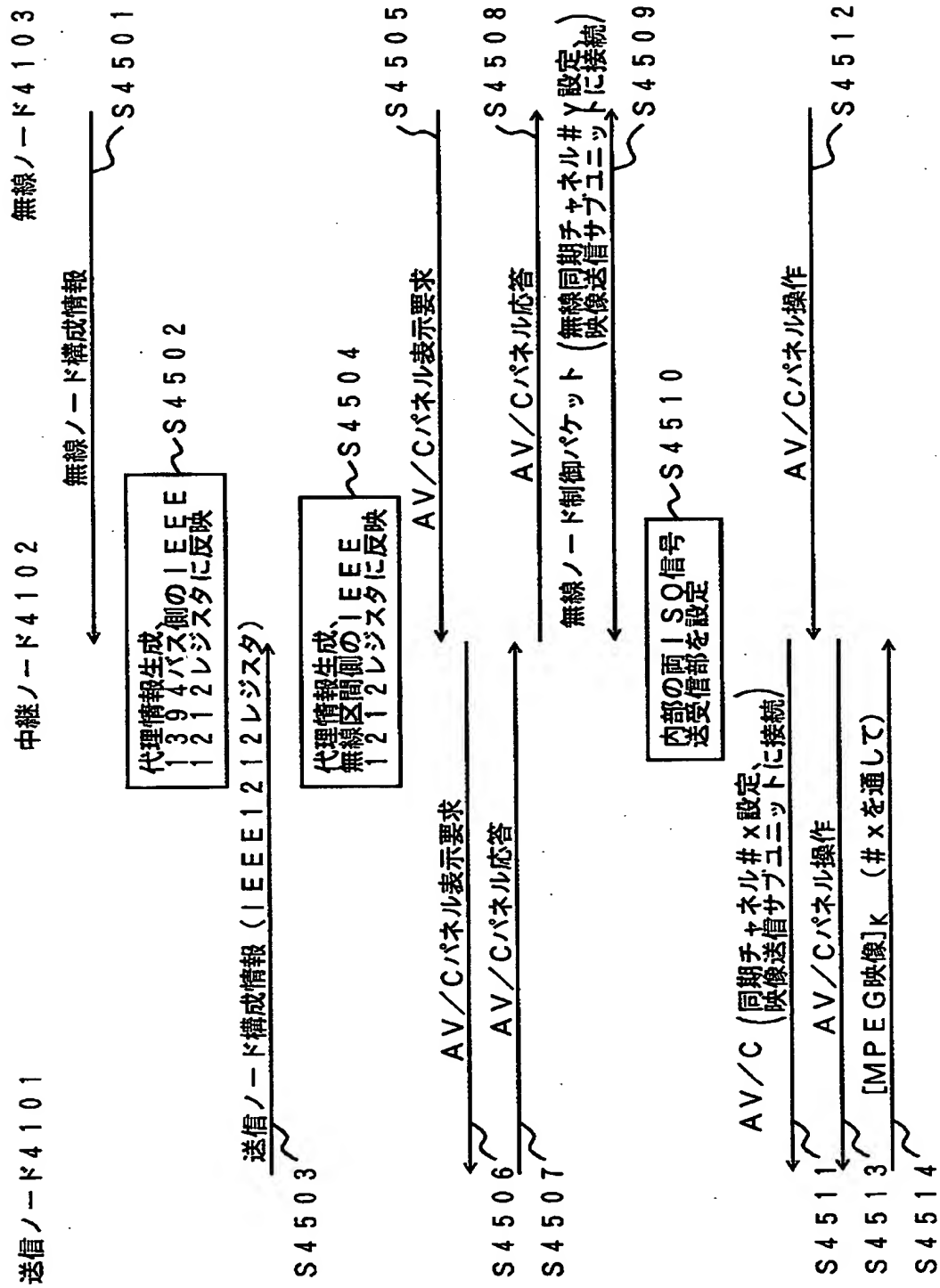
【图 3 9】



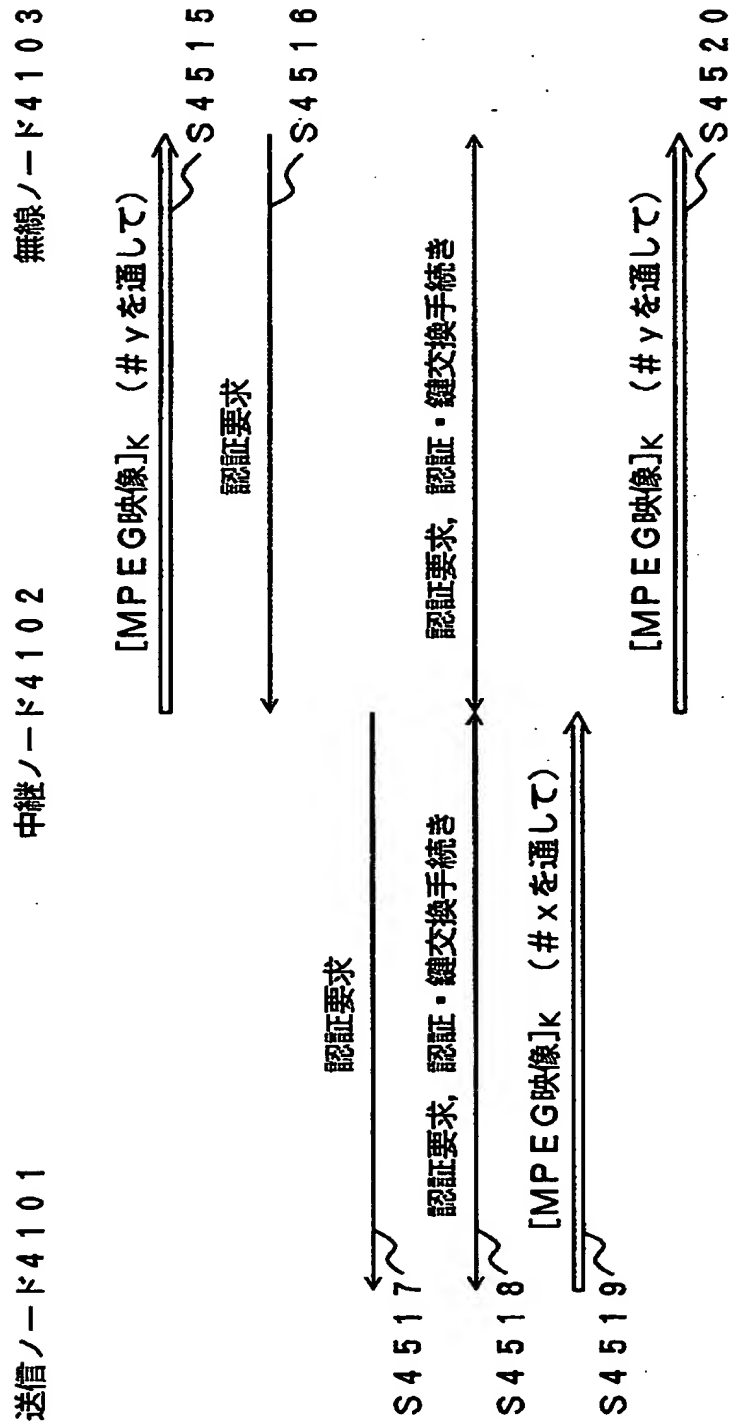
【図 40】



【図 4 1】



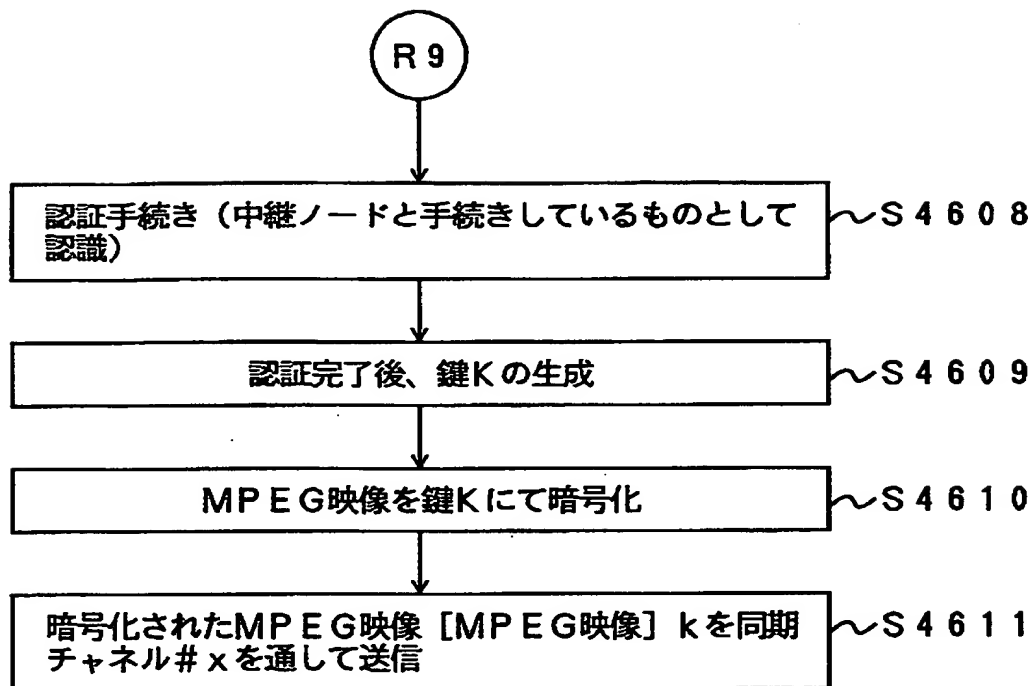
【図 4 2】



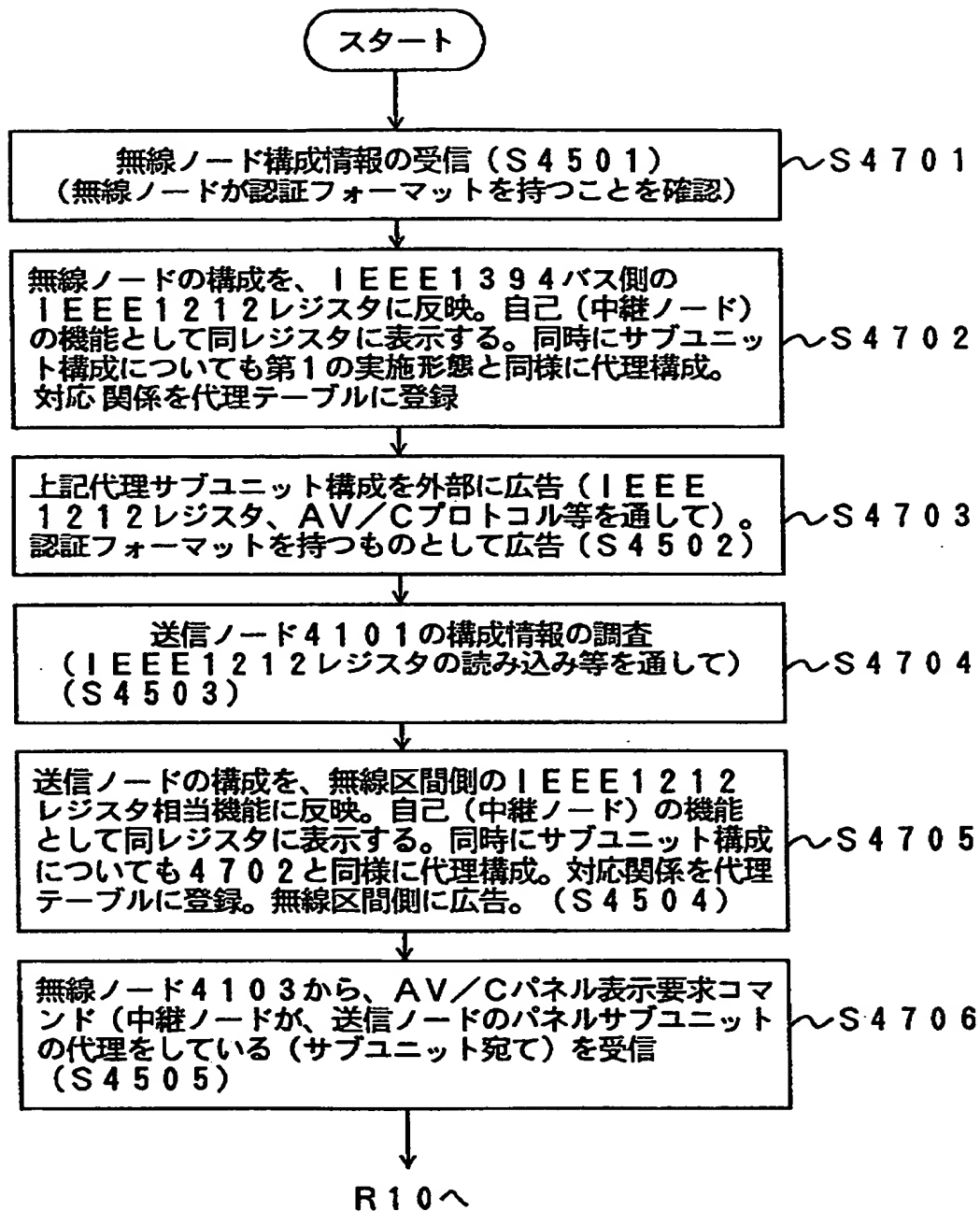
【図 43】



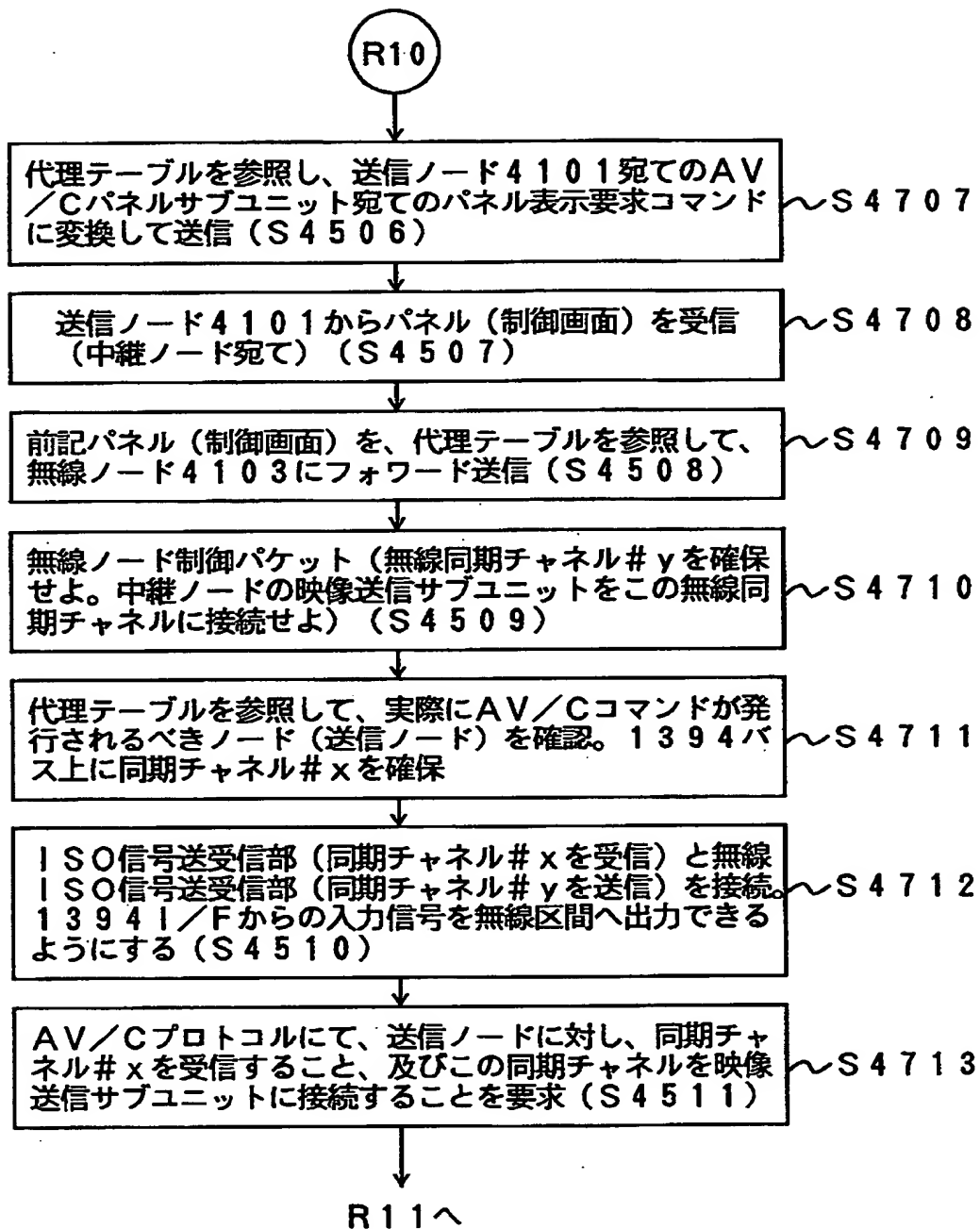
【図 4 4】



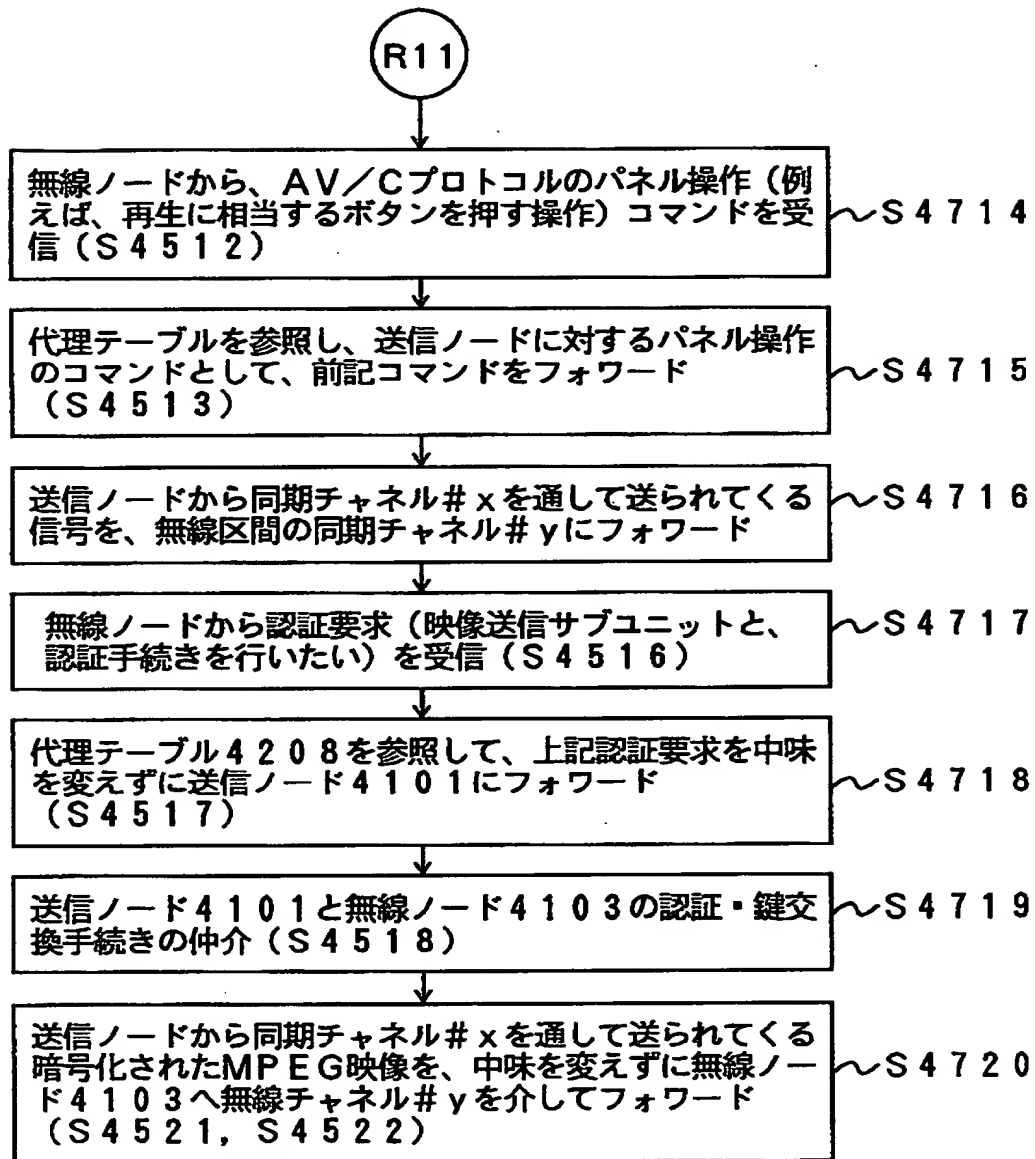
【図 45】



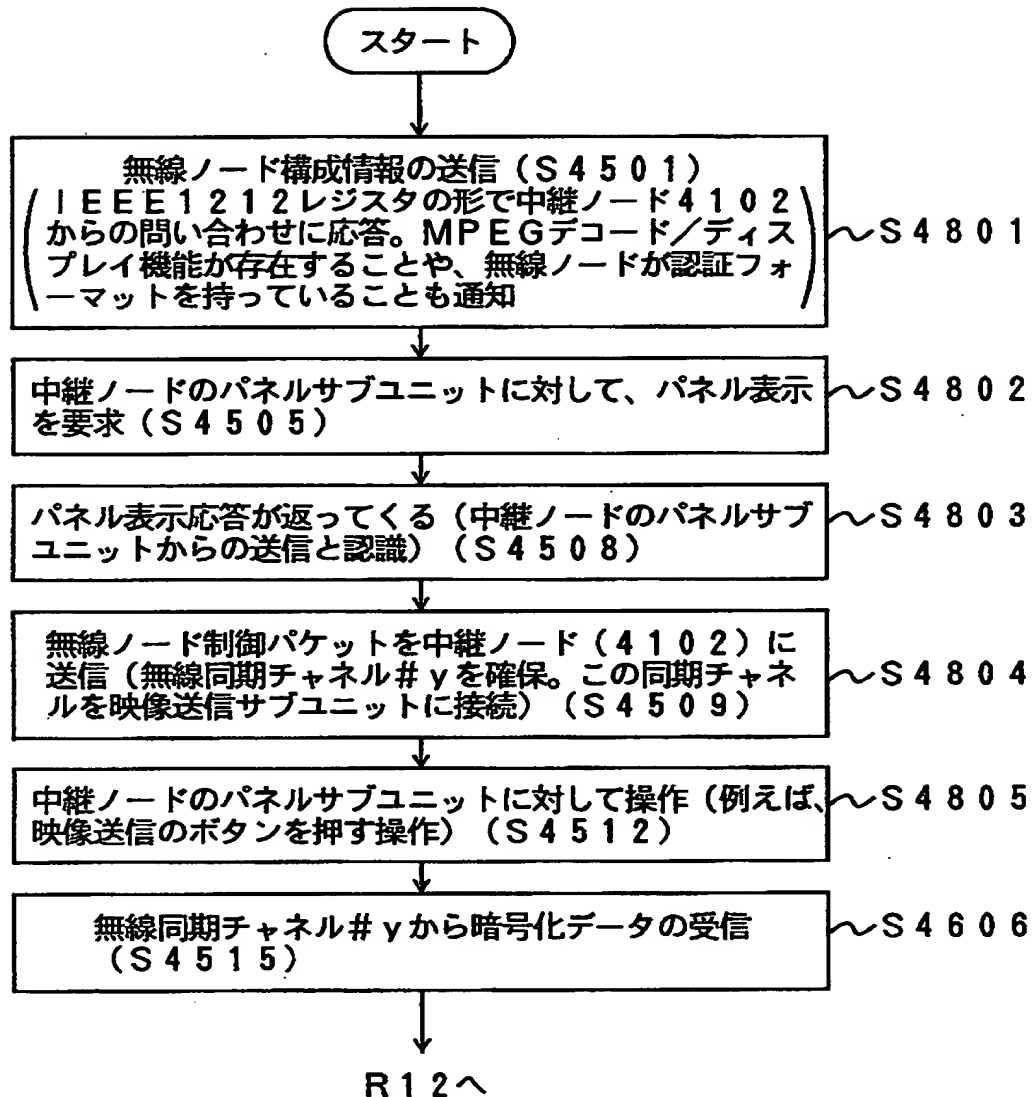
【図 4 6】



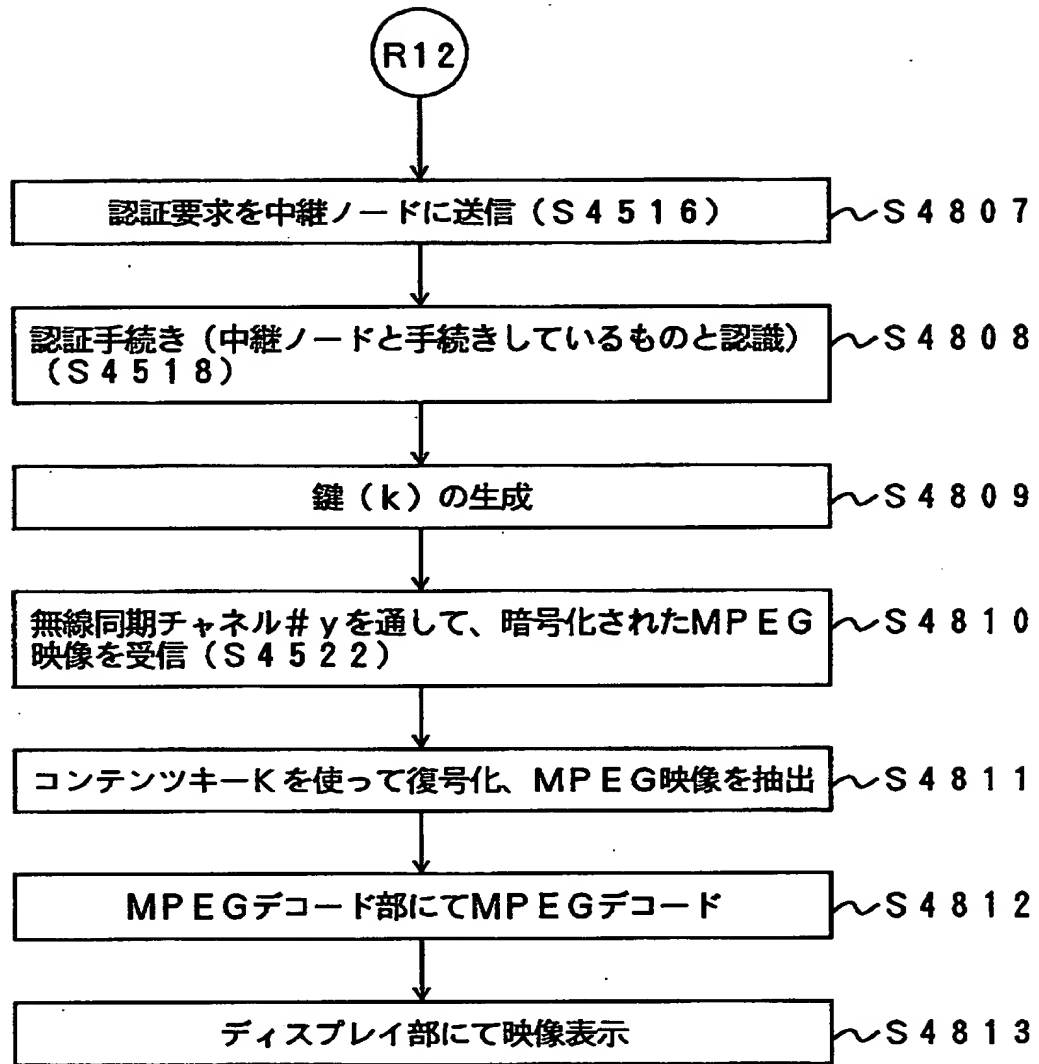
【図 47】



【図 48】



【図 49】



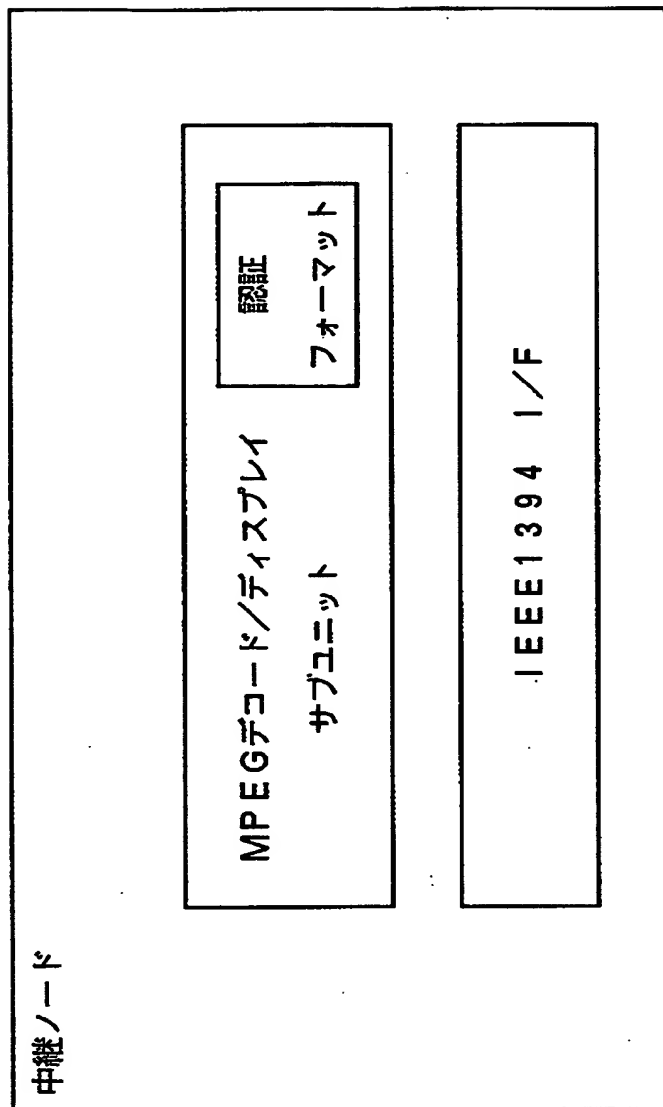
【図 50】

無線区間側の実体	中継ノードが1394側に代理サービスする形態
無線ノード4103の MPEGデコード/ディスプレイ機能 (認証フォーマット有)	MPEGデコード/ディスプレイサブユニット (認証フォーマット有)
無線ノード4103のパネル機能	パネルサブユニット
...	...

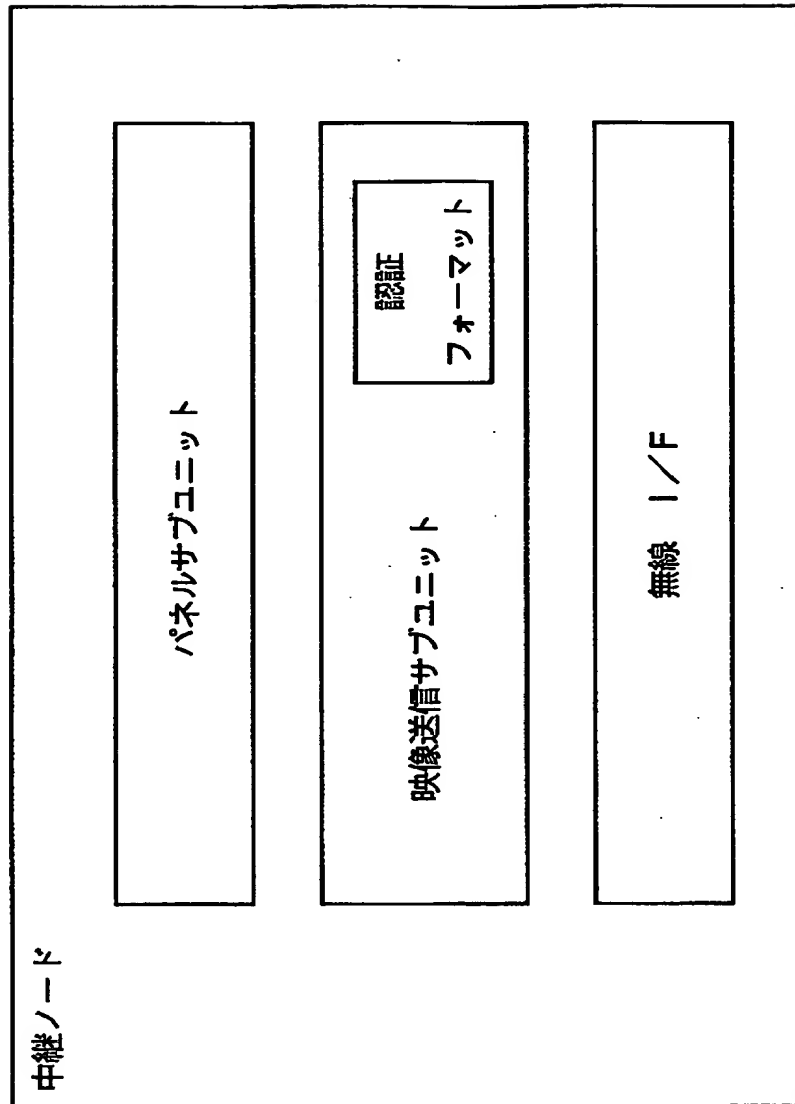
【図 51】

1394バス側の実体	中継ノードが無線区間側に代理サービスする形態
送信ノード4101の映像送信サブユニット (認証フォーマット有)	映像送信サブユニット (認証フォーマット有)
送信ノード4101のパネルサブユニット	パネルサブユニット
...	...

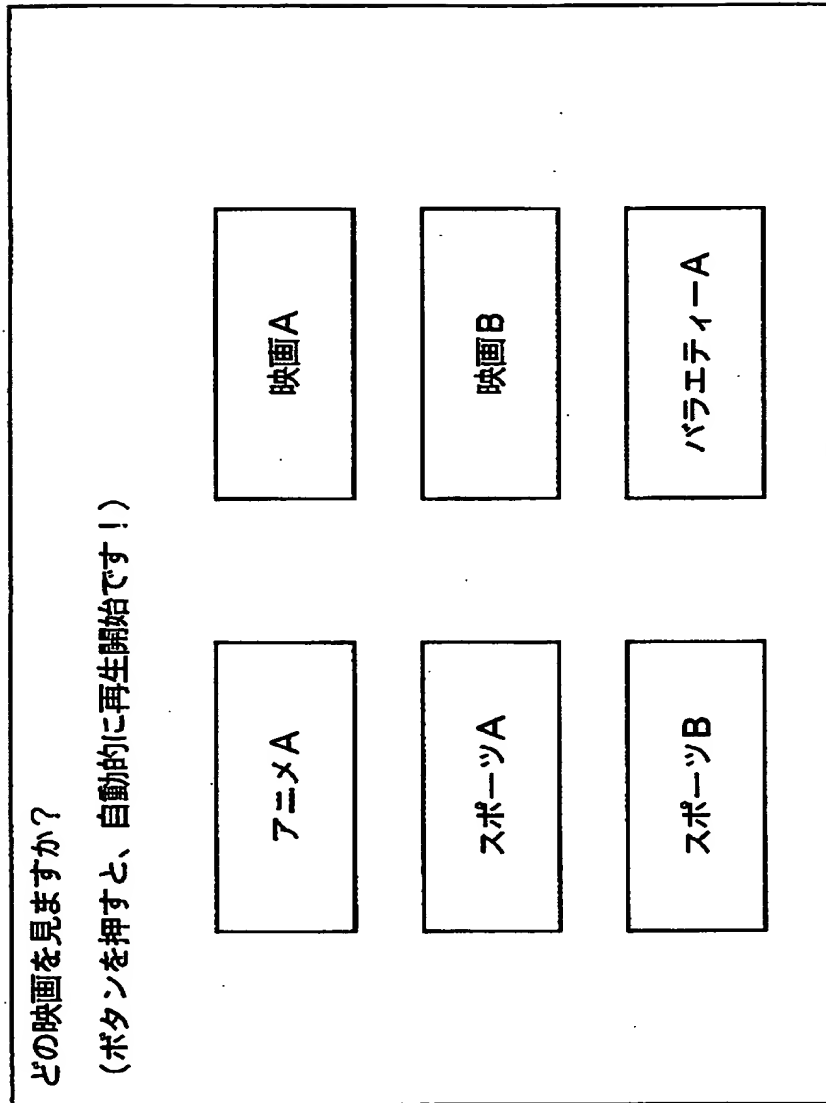
【図 52】



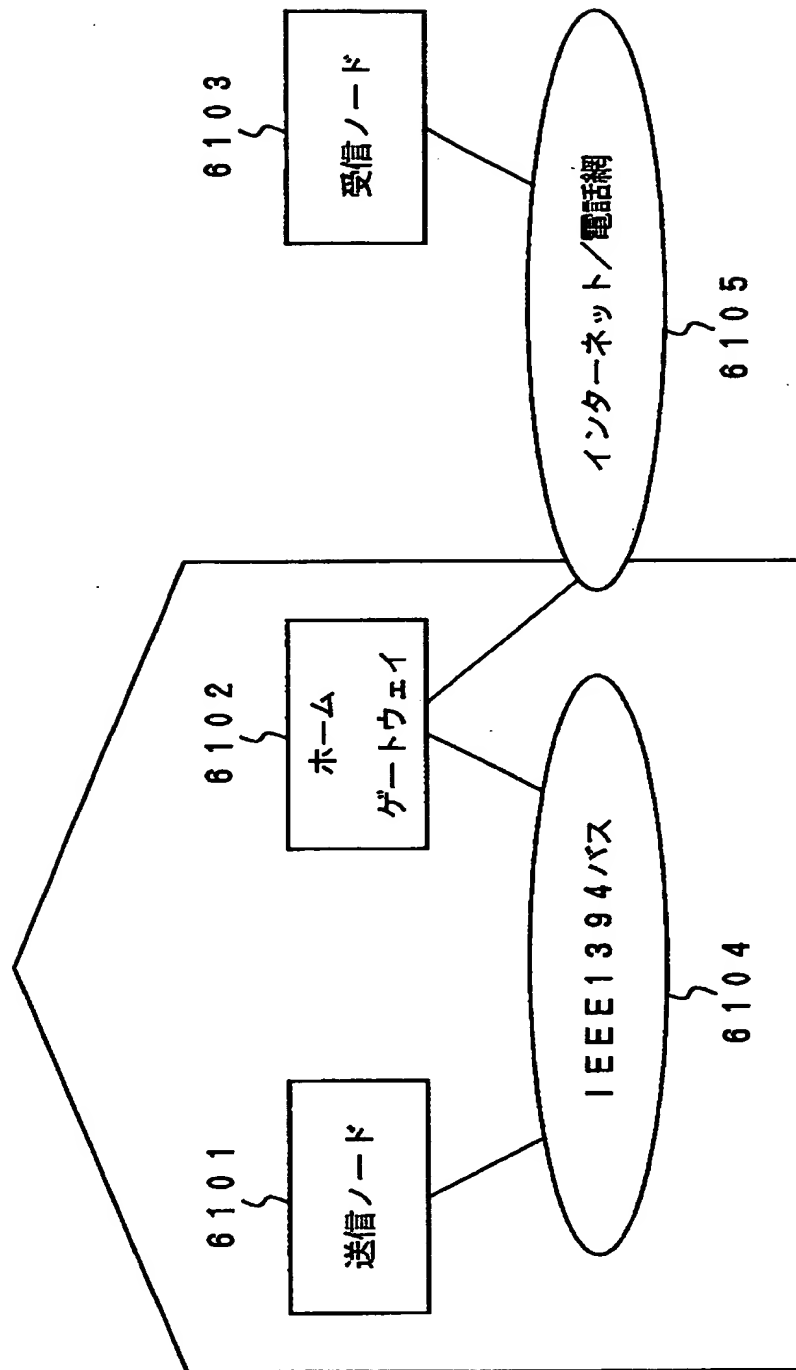
【図 53】



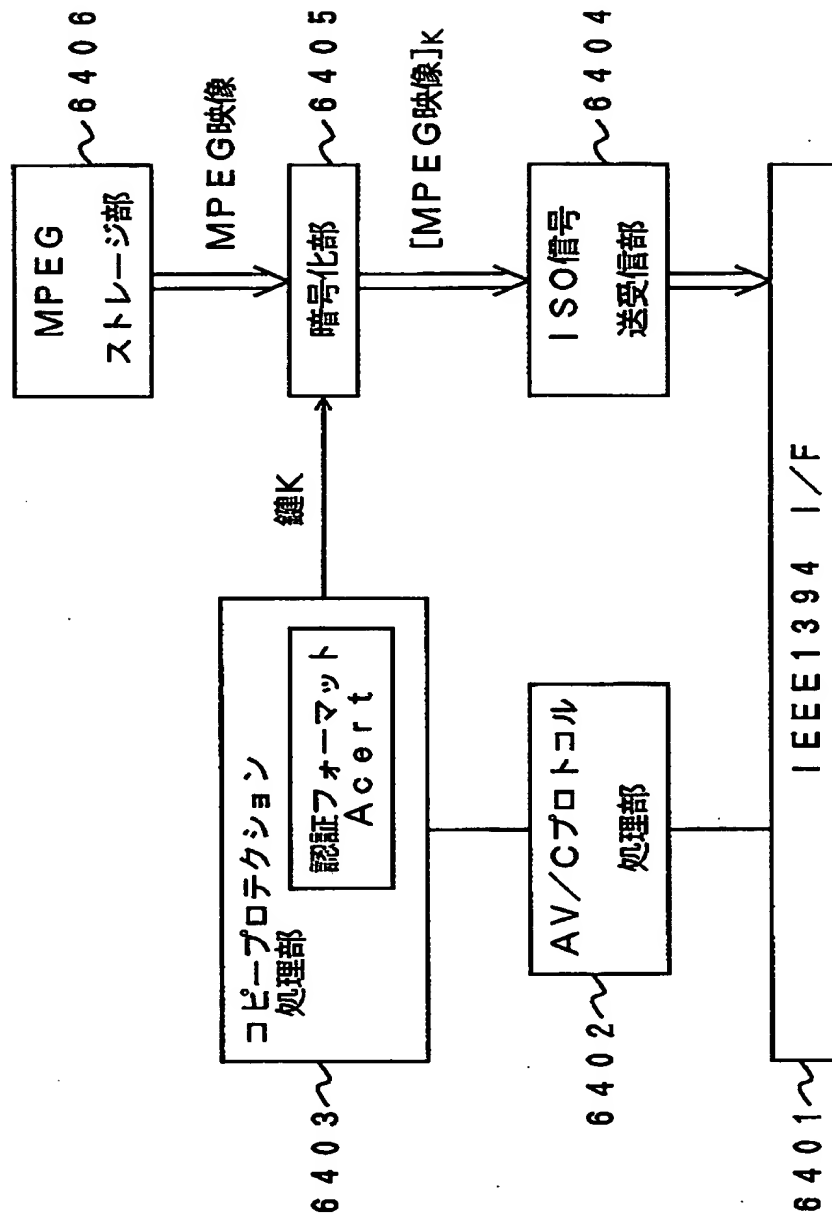
【図 54】



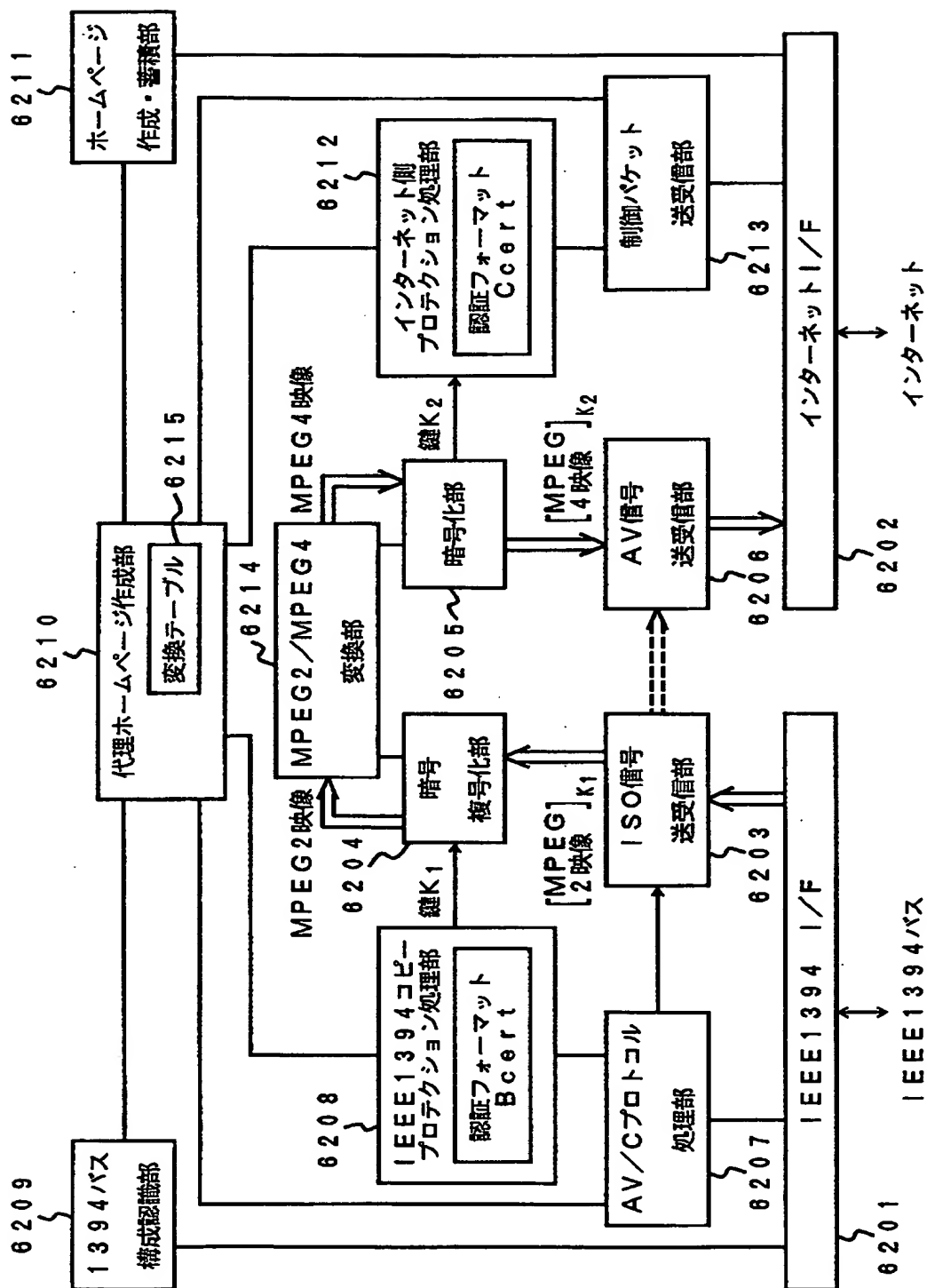
【図55】



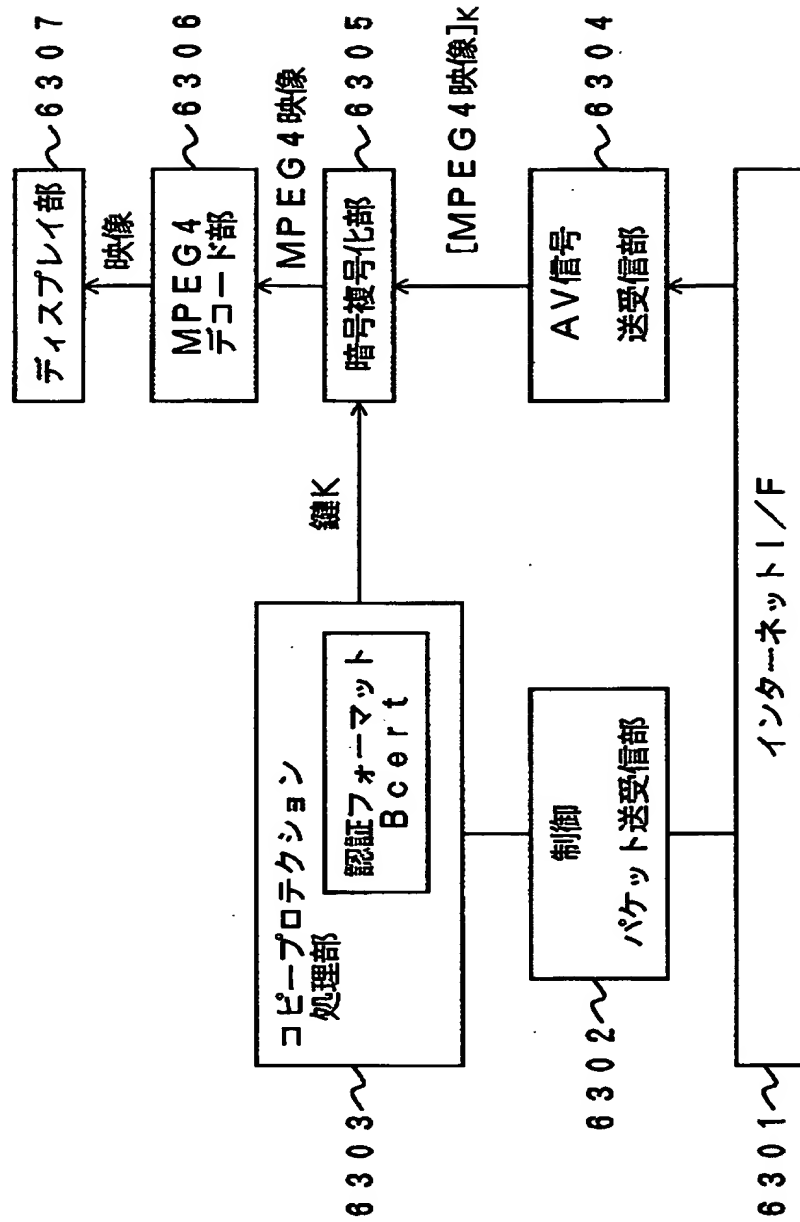
【図 56】



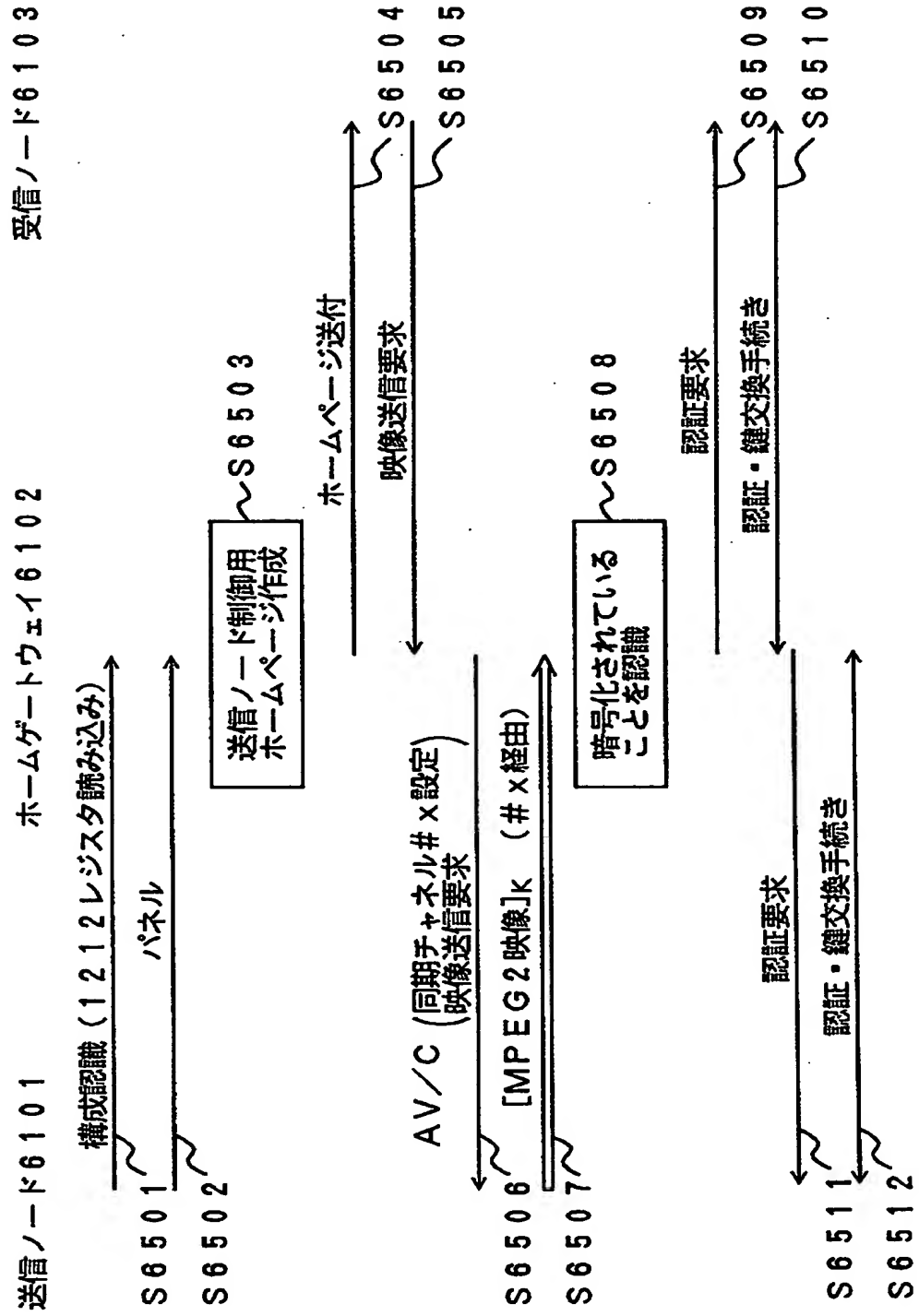
【图 5 7】



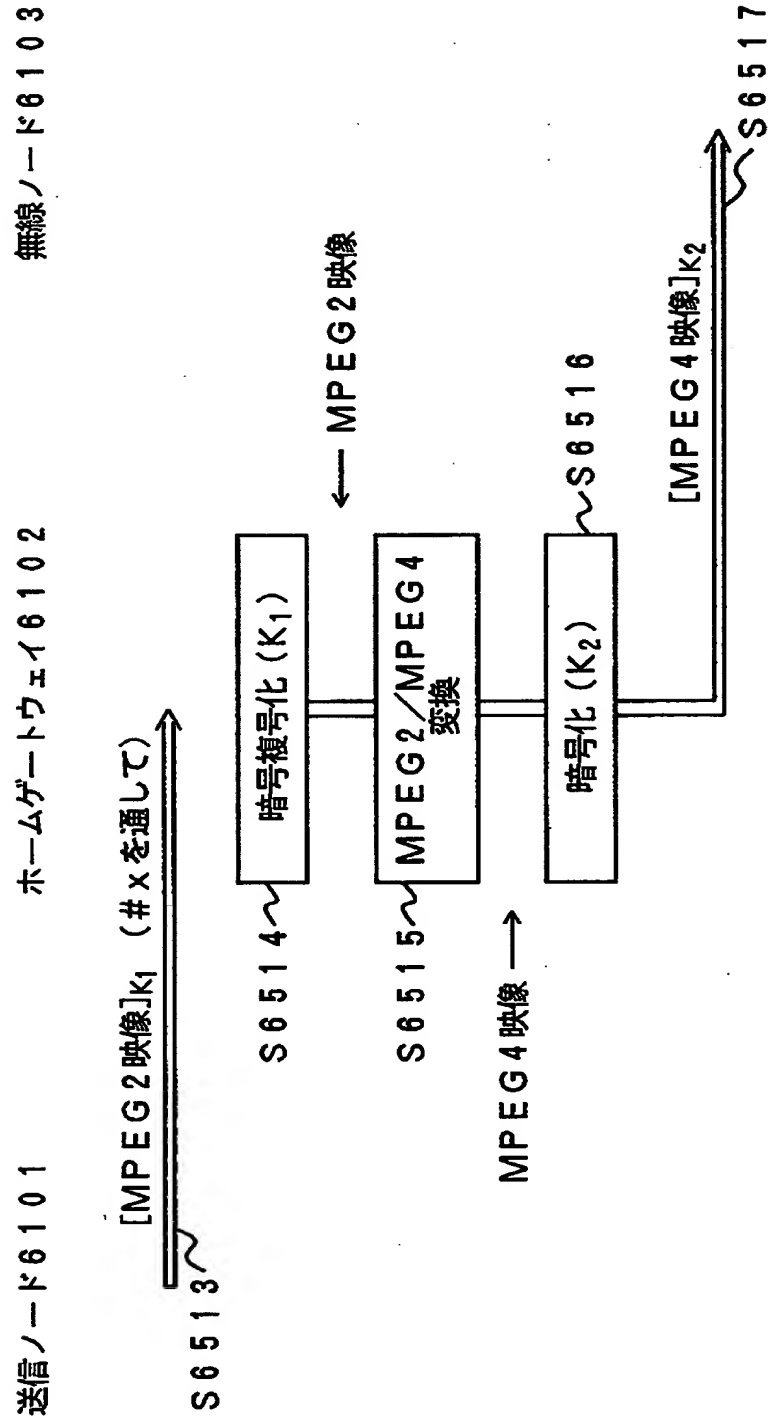
【図 58】



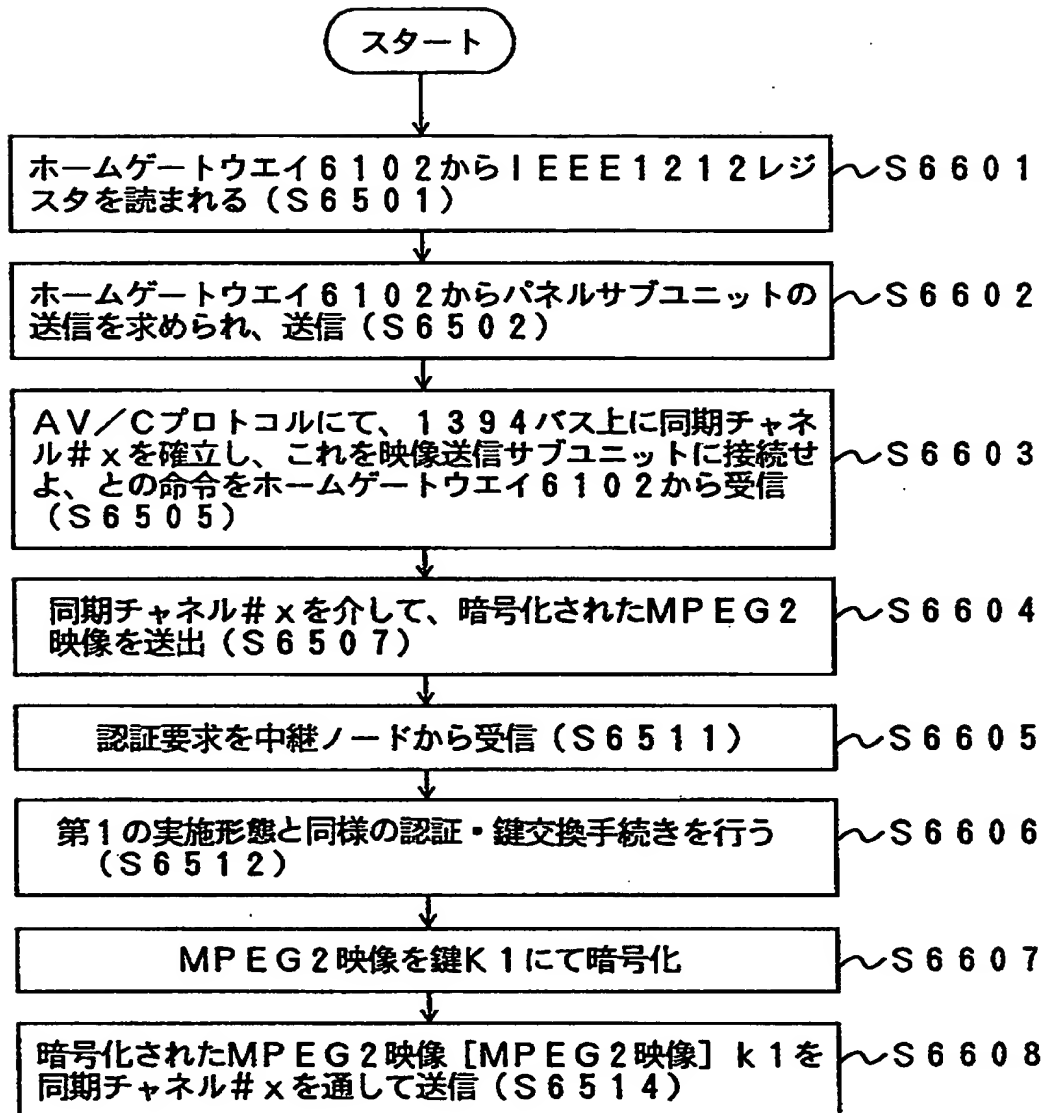
【図59】



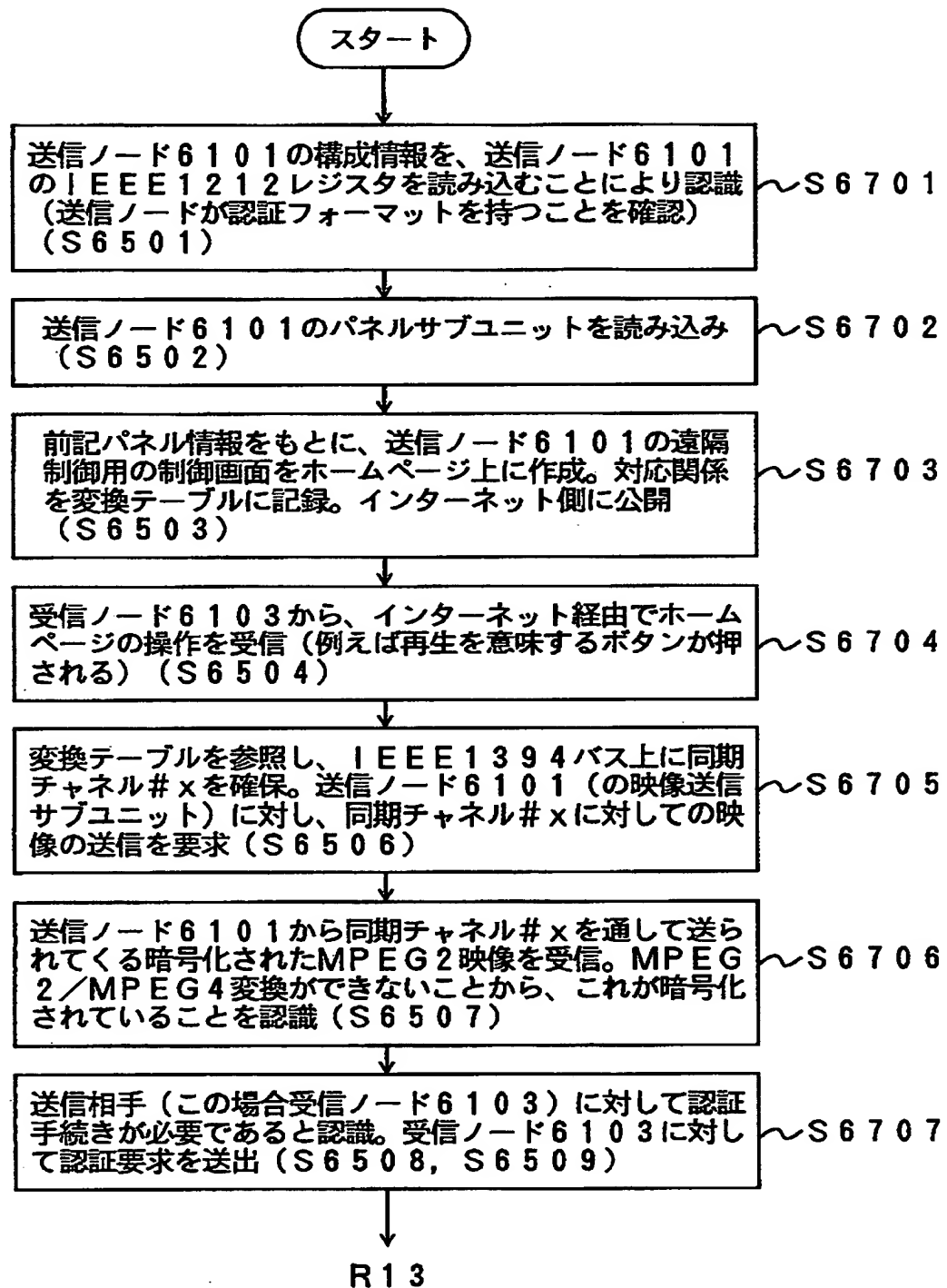
【図 60】



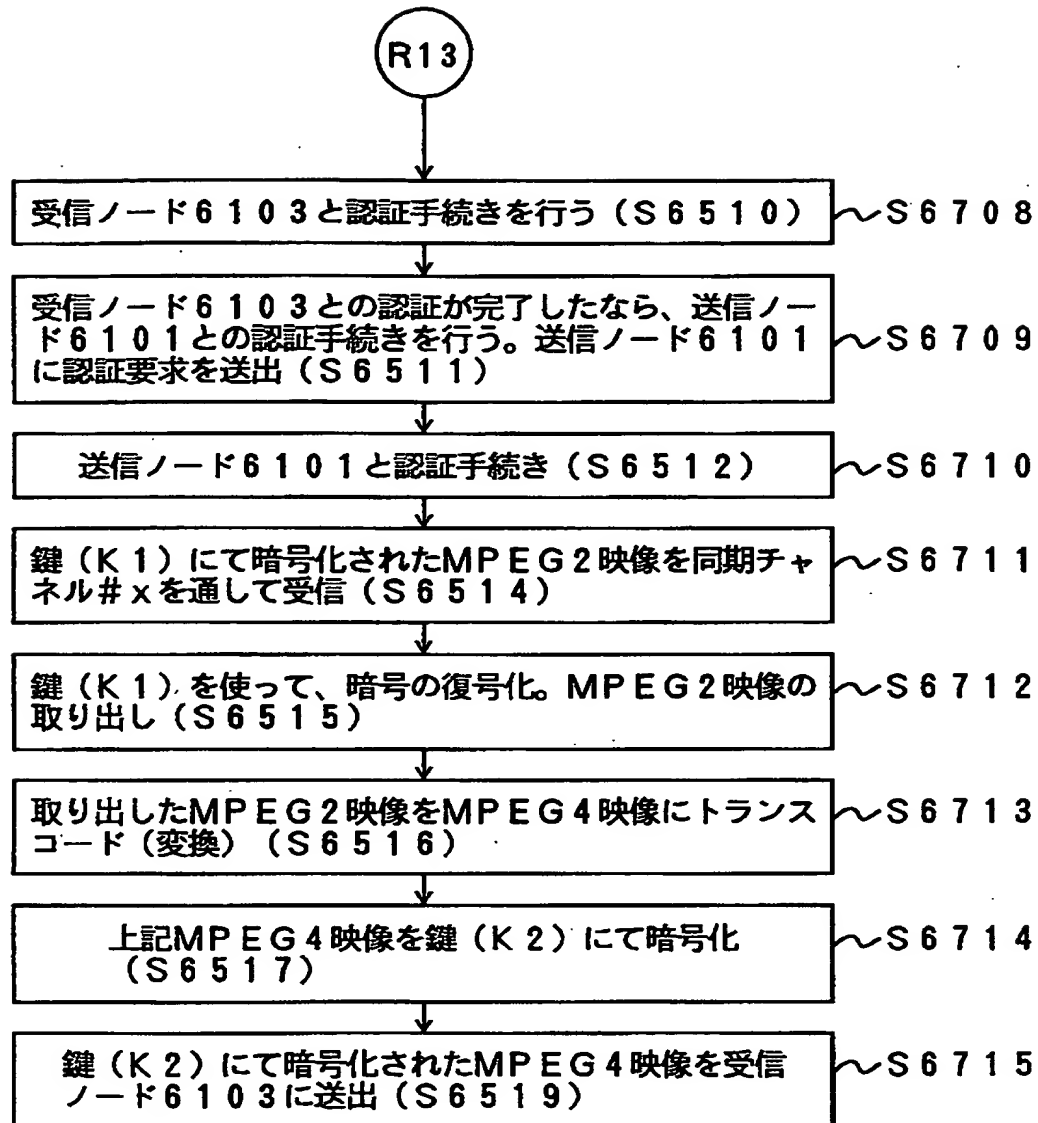
【図 61】



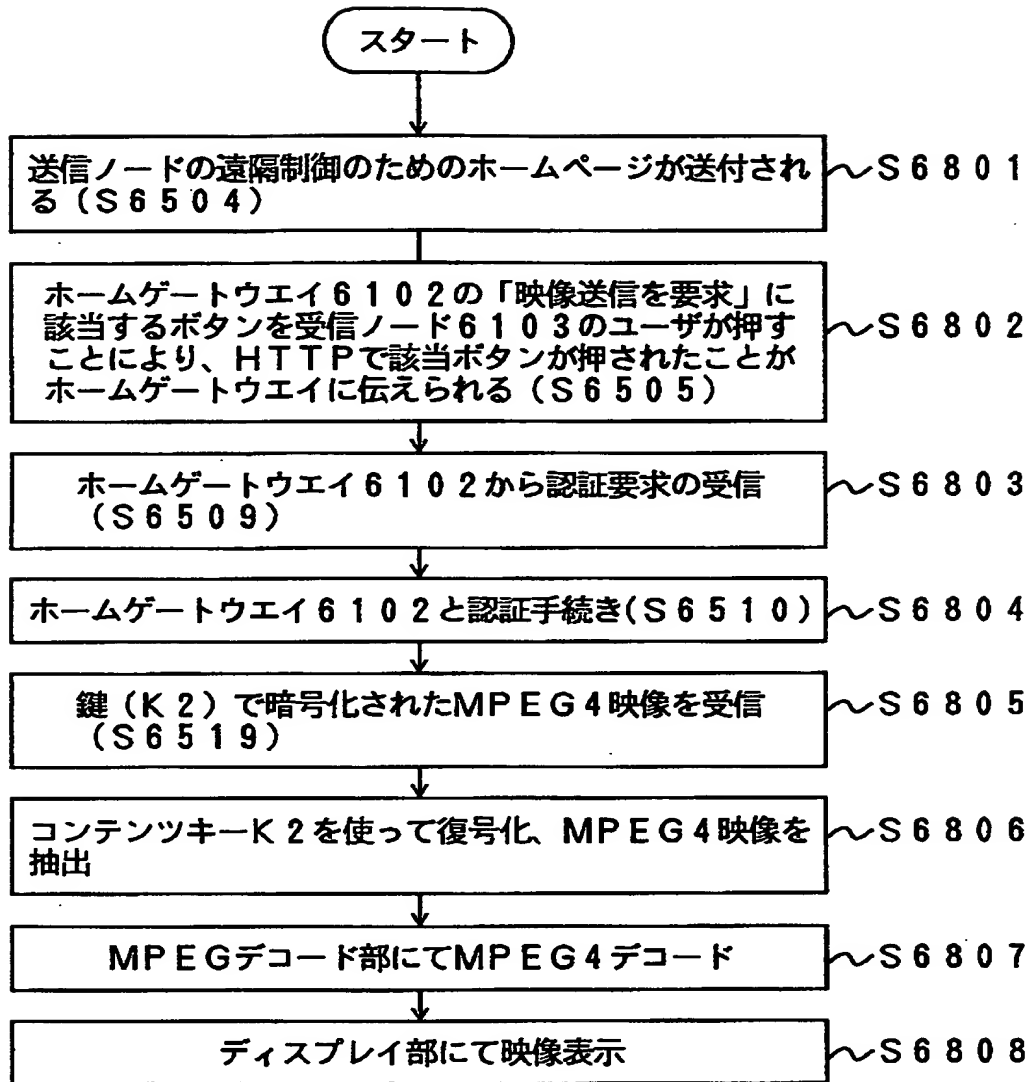
【図 62】



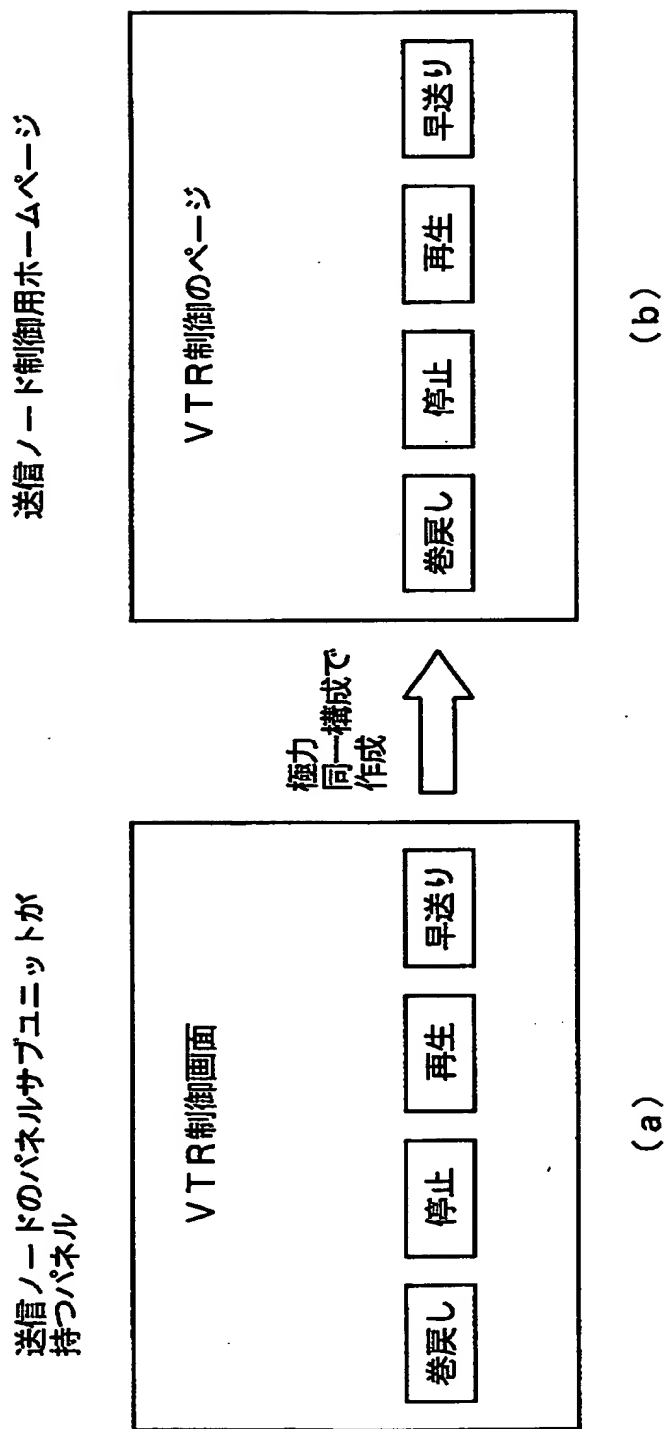
【図 63】



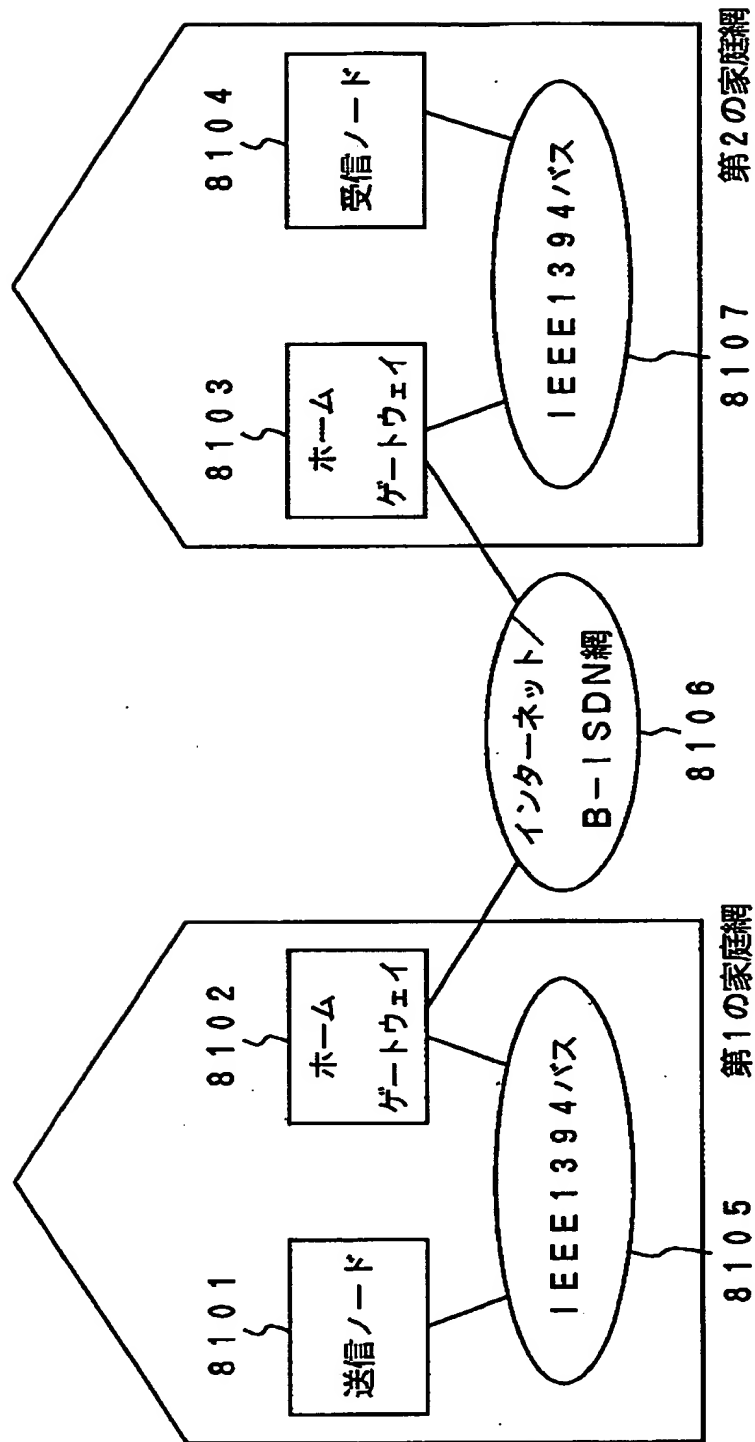
【図 64】



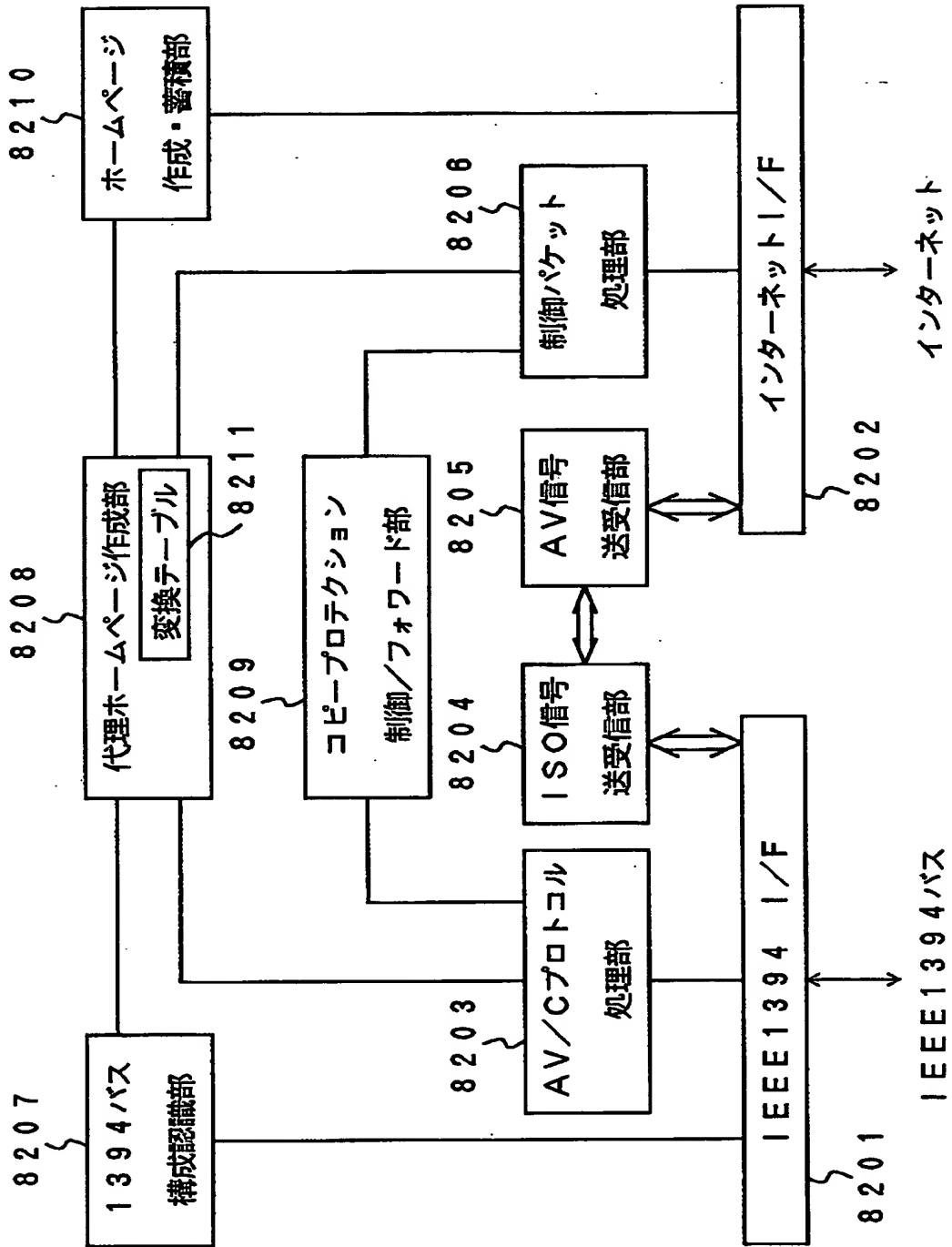
【図 65】



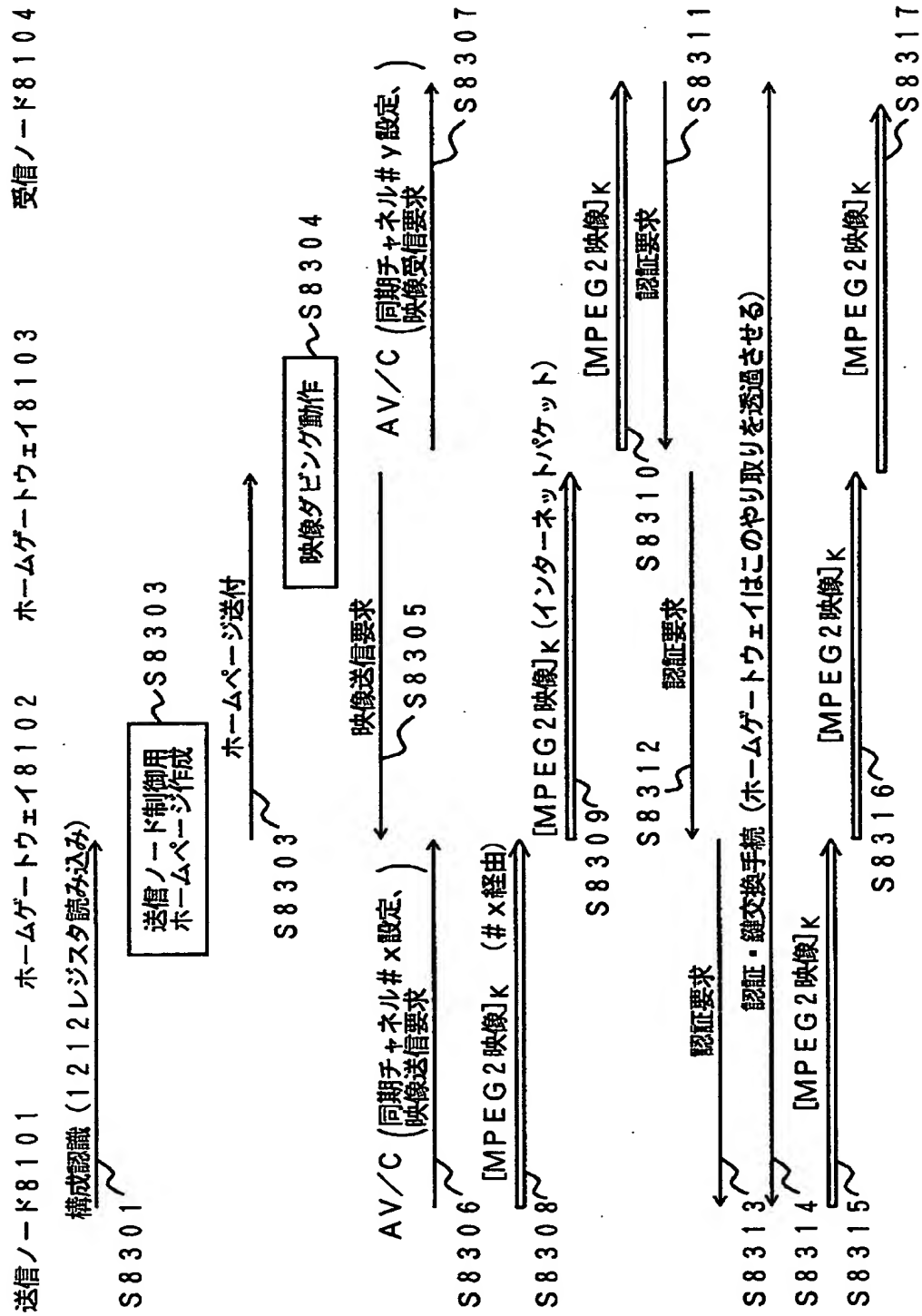
【図66】



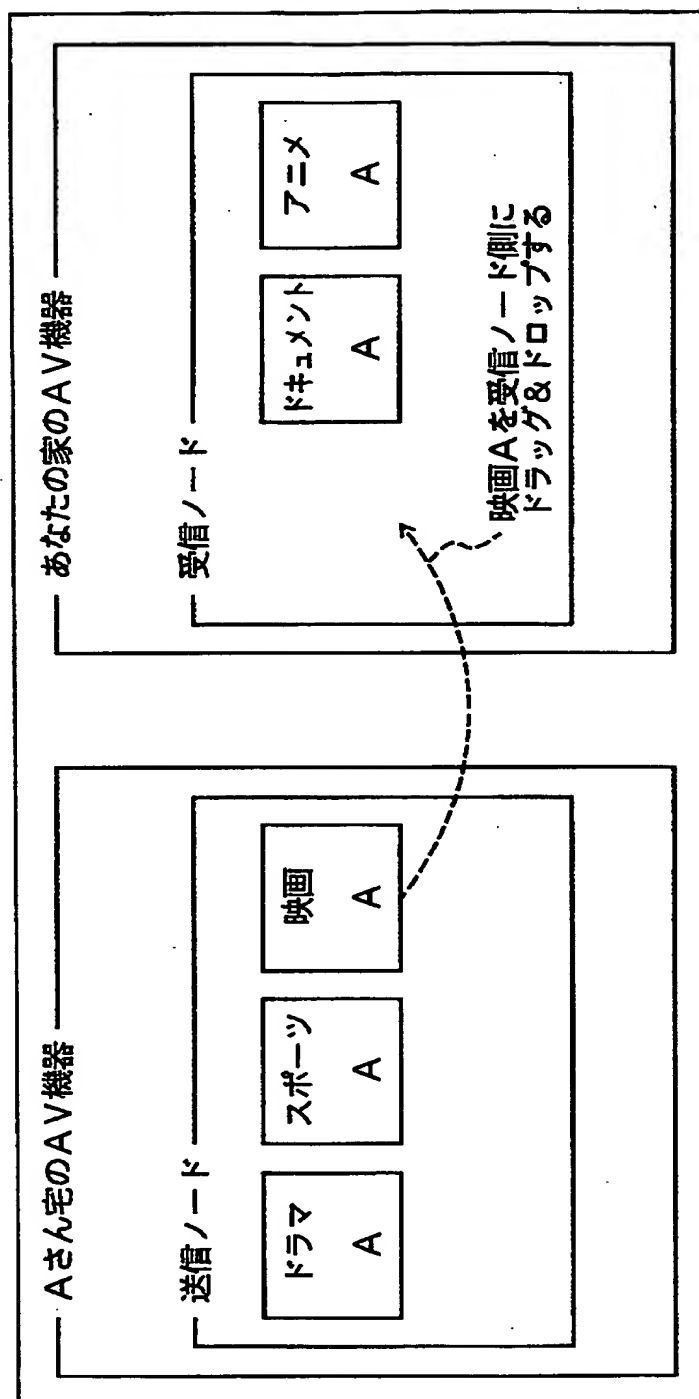
【図 67】



【図 68】



【図 69】



【書類名】 要約書

【要約】

【課題】 同じネットワークには接続されていない装置間のコンテンツ保護手続きを可能とする中継装置を提供すること。

【解決手段】 第1のネットワークに接続されたインタフェースと、第2のネットワークに接続されたインタフェースと、第2のネットワーク上の装置又はサービス又はサブユニットを自中継装置上のものとして第1のネットワーク側に開示し、この装置又はサービス又はサブユニット宛の第1の情報を代理で受信し、該第2のネットワーク上の装置又はサービス又はサブユニットへの第2の情報に変換して送信する代理構成機能と、第1のネットワーク上の装置からの第1の情報を受信した際この情報が少なくとも所定の情報であるか否かを検出する機能と、検出した第1の情報が所定の情報であった場合にはこの所定の情報を第2のネットワーク上の装置又はサービス又はサブユニットに転送する機能とを有する。

【選択図】 図1

【書類名】 職権訂正データ  
【訂正書類】 特許願

<認定情報・付加情報>

【特許出願人】

【識別番号】 000003078

【住所又は居所】 神奈川県川崎市幸区堀川町 7 2 番地

【氏名又は名称】 株式会社東芝

【代理人】 申請人

【識別番号】 100058479

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 鈴江 武彦

【選任した代理人】

【識別番号】 100084618

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内

【氏名又は名称】 中村 誠

【選任した代理人】

特平 10 - 292824

【識別番号】 100070437  
【住所又は居所】 東京都千代田区霞が関 3 丁目 7 番 2 号 鈴榮内外國  
特許法律事務所内  
【氏名又は名称】 河井 将次

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日

[変更理由] 新規登録

住 所 神奈川県川崎市幸区堀川町72番地  
氏 名 株式会社東芝